目　　录

第 1 章 代数的起源

代数从何而来？粗略地说，代数起源于加法，乘法和求整数次方幂的计算艺术．如果用字母代替数 (这一点并非显而易见且有多种方式)，就使我们能够在更广泛的代数系统中使用类似的法则进行计算．对这一问题给出透彻回答的尝试将我们带进了久远的时代，带进了数学思想奇妙产生的过程．这一答案，最困难的部分与我们今天的基本代数结构：群、环、域、模等紧密相关．但这恰好是本书的大部分内容，因而第一章的目的目前似乎还达不到．

幸运的是，在大多数代数公理抽象的外表下，隐含着非常具体的理论和实际问题，它们的解决常常幸运地成为进一步发展抽象理论的动力．同样地，所发展的理论又成为解决这些问题的基础和工具．存在于所有数学领域内的理论与应用之间的复杂的相互作用在代数中表现得尤为明显，同时也在某种程度上说明我们通常采用的围绕中心问题层层深入的教学方法是有道理的．

在对历史事件进行过简短评注之后，我们将叙述包含在下面章节中的一些问题．这些问题之一成为研究线性方程组，矩阵和行列式理论的出发点．我们介绍高斯方法并得到解线性方程组的初步认识．

在这一步引入标准的符号和术语是有益的，为此我们将扼要地给出集合与映射的理论．

我们将引入等价关系和商映射的重要概念．进一步，为了详细讲解数学归纳法原理．建立了一些初等的组合关系式，我们特别引出了置换的概念，它是行列式理论的基础．

最后在末尾一节中列出了整数的最简单的算术性质．这些性质不仅将来要用，也是在更复杂的代数系统中构造类似算法的原型．

本章的材料并未超出中学课程太多. 仅要求读者准备上升到更高更一般的观点. 学生可以从 §3 开始读起.

§1 简谈代数

在我们今天的时代, 谈论数学的 "代数化" 不是没有理由的, 即代数的思想和方法渗透到数学各个分支的理论与应用中. 这种情况在 20 世纪中叶变得十分明显, 但情况并不总是如此. 正如人类活动的所有领域一样, 数学也会受到时尚的影响. 代数方法的流行有其实际的原因, 尽管对它的迷恋有时会超越理智的界限. 由于掩盖了内容的代数外壳不亚于对代数的基本无知造成的不幸, 所以教科书的作者要是擅长于避免代数过分的形式化, 那么就会合情合理地受到赞许.

只要不走极端, 代数自古以来就是数学的一个重要的组成部分. 几何也是这样, 但我们愿意在这里引用索菲 · 格尔曼的观点. "代数不外是符号的几何, 而几何不外是图形的代数." 后来情况有些变化, 但仍可以说 "数学对象的自然属性实质上是不太重要的第二位的事情, 例如我们得到的结果既可以用纯几何定理的形式表述, 也可以借助解析几何以代数定理的形式出现."(尼 · 布尔巴基).

根据 "重要的不是数学对象, 而是它们之间的关系" 这一原则, 代数被定义为对各种集合的元素施行代数运算的科学 (这种说法有些重复, 并且使未入门者完全莫名其妙). 代数运算本身源于初等算术. 反过来, 基于代数学的思想, "高等算术", 即数论中的许多事实得到了最自然的证明.

但是代数结构, 即带有代数运算的集合, 意义远远超出了对数论的应用. 许多数学对象 (拓扑空间, 多复变函数等等), 其研究方法是建立相应的代数结构, 即便与所研究的对象不完全吻合, 但在所有的情况下都能反映出它们的本质方面. 在现实世界中没有什么东西是完全相同的.

对代数学的这一明确看法是在 45 年前由量子力学的创始人之一狄拉克提出来的, 他说: "现代物理学越来越需要抽象数学及其基础的发展. 非欧几何和非交换代数一度被认为是虚构的, 是迷恋逻辑推理的简单结果, 而现在则被公认为是描绘物理世界不可或缺的工具."

代数工具在研究量子力学的基本粒子, 在考察刚体性质和晶体结构 (在这方面, 群表示理论特别重要), 在分析经济模式, 在制造现代化计算机等方面都是非常有用的.

与此同时, 代数学也受到其他学科新鲜汁液的哺育, 其中包括数学中的其他学科. 例如代数的同调方法产生于拓扑学和代数数论. 因而代数的面貌和人们对代数的看法在不同的时期有所改变是不足为奇的. 我们不可能详细地列出这些变化, 不仅由于篇幅有限, 尤其是因为书写历史必需具体, 而这只有在学习了代数的基础知识之后才能办到. 我们仅限于列举一个带有人名和年代的图表.

古代巴比伦和埃及文化，希腊文化. 丢番图的“算术”(公元前3世纪)	自然数与正有理数的四则运算. 几何学与天文学中的代数公式. 作图问题的形成(立方倍积与三等分角)，代数思想的使用是很久以后的事情.
中世纪的东方文化. 穆罕默德·花拉子米(Muhammad al-Khwārizmī)的著作《代数》(约825年)	一次及二次代数方程. 术语“代数”一词的产生.
文艺复兴时代 S. 费罗(1465—1526) N. 塔尔塔利亚(1500—1557) G. 卡尔达诺(1501—1576) L. 费拉里(1522—1565) F. 韦达(1540—1603) R. 邦贝利(1530—1572)	三次和四次代数方程的一般解. 建立了现代的代数符号.
17至18世纪 R. 笛卡儿(1596—1650) P. 费马(1601—1665) I. 牛顿(1643—1727) G. 莱布尼茨(1646—1716) L. 欧拉(1707—1783) J. 达朗贝尔(1717—1783) J. L. 拉格朗日(1736—1813) G. 克拉默(1704—1752) P. 拉普拉斯(1749—1827) A. 范德蒙德(1735—1796)	出现了解析几何——几何与代数之间的坚实的桥梁. 数论研究趋于活跃. 开始研究多项式代数. 深入研究代数方程求解的一般公式. 证明数值系数代数方程根的存在性的首批方法. 行列式理论的开端.
19世纪至20世纪初 K. F. 高斯(1777—1855) P. 狄利克雷(1805—1859) E. 库默尔(1810—1893) L. 克罗内克(1823—1891) R. 戴德金(1831—1916) E. L. 佐洛塔廖夫(1847—1878) G. F. 沃罗诺依(1868—1908) A. A. 马尔可夫(1856—1922)	证明数值系数方程根的存在性的基本定理. 代数数论的深入发展.
P. L. 切比雪夫(1821—1894) C. 埃尔米特(1822—1901) N. I. 罗巴切夫斯基(1792—1856) A. 胡尔维茨(1859—1919)	探讨代数方程近似解的求法. 使根处于某一位置时系数应满足的条件.

续表

P. 鲁菲尼(1765—1822) N. H. 阿贝尔(1802—1829) C. 雅可比(1804—1851) E. 伽罗瓦(1811—1832) G. 黎曼(1826—1866) A. L. 柯西(1789—1857) C. 若尔当(1838—1922) L. 西罗(1832—1918)	证明次数≥5 的一般方程不能用根式求解. 代数函数论的发展. 伽罗瓦理论的创立. 主要基于置换群的有限群论的开端.
H. 格拉斯曼(1809—1877) J. 西尔维斯特(1814—1897) A. 凯莱(1821—1895) W. 哈密尔顿(1805—1865) G. 布尔(1815—1864) S. 李(1842—1899) F. 弗罗贝尼乌斯(1849—1918) J. 塞雷(1819—1885) M. 诺特(1844—1922) D. A. 格拉韦(1863—1939) H. 庞加莱(1854—1912) F. 克莱茵(1849—1925) W. 伯恩赛德(1852—1927) F. 莫林(1861—1941) J. 舒尔(1875—1941) H. 外尔(1885—1955) F. 恩里克(1871—1946)	线性代数方法的深入发展. 发现四元数后引起的超复数的研究 (这样的系统现在称为代数). 特别是连续群(李群)的发展为李代 数理论奠定了基础. 代数几何和不变量理论成为数学的重要 分支. 在 19 世纪, 数学尚未高度专门化, 许多大科 学家在不同的领域内创造性地工作.
J. 冯·诺依曼(1903—1957) D. 希尔伯特(1862—1943) E. 嘉当(1869—1951) K. 亨泽尔(1861—1941) E. 施泰尼茨(1871—1928) E. 诺特(1882—1935) E. 阿廷(1898—1962) H. 布尔巴基《数学原理》.	20 世纪上半叶, 整个数学大厦得到了根本 性的改造. 代数不再是关于解代数方程的科学, 开始 坚定地沿着公理化和更加抽象的道路发展.
环、模、范畴、同调理论成为常用的语言. 许多不同的理论符合泛代数的通用模式. 模型论兴起于代数与数理逻辑的交界处. 古老的理论焕然一新, 扩大了自己的应用领域. 例子有现代代数几何、代数拓扑、代数K–理论、代数群理论. 有限群论经历了特殊的飞跃.	

目前代数学正处在生机勃勃的发展中. 其中俄罗斯数学家做出了重大贡献. 我国高水平的代数研究, 应归功于下述学者, 如 N.G. 切博塔廖夫 (1894—1947), O.Ju. 施米特 (1891—1956), A.I. 马尔采夫 (1909—1967), A.G. 库洛什 (1908—1971), P.S. 诺

维科夫 (1901—1975), D.K. 法捷耶夫 (1907—1989).

§2 几个典型问题

本节列出水平各异的四个问题，前三个问题互不相同，用于引起对不同类型的域，对线性空间，对群及其表示的研究，它们的代数理论将要在下面谈到. 许多专门著作是为了"解答"这类问题而写的. 第四个问题是为了引出线性方程组的研究，读者不看后面解线性方程组一节的内容，自己试着去解决它是有益处的.

1. 方程的根式解问题 从初等代数已知求二次方程 $ax^2+bx+c=0$ 的解 x_1, x_2 的公式

$$x_{1,2}=\frac{-b\pm\sqrt{b^2-4ac}}{2a}. \tag{1}$$

在三次方程

$$x^3+ax^2+bx+c=0$$

中，用 $x-\frac{a}{3}$ 替换 x, 得到形如 $x^3+px+q=0$ 的方程. 方程的三个根 x_1,x_2,x_3 可由它的系数表示成下述形式. 若令

$$\begin{aligned} &D=-4p^3-27q^3,\quad \varepsilon=\frac{-1+\sqrt{-3}}{2},\\ &u=\sqrt[3]{-\frac{27}{2}q+\frac{3}{2}\sqrt{-3D}},\quad v=\sqrt[3]{-\frac{27}{2}q-\frac{3}{2}\sqrt{-3D}} \end{aligned} \tag{2}$$

(立方根满足 $uv=-3p$), 则可证明

$$x_1=\frac{1}{3}(u+v), x_2=\frac{1}{3}(\varepsilon^2u+\varepsilon v), x_3=\frac{1}{3}(\varepsilon u+\varepsilon^2 v). \tag{3}$$

与公式 (1) 一样，对字母系数 a,b,c,p,q 的任意数值，例如任意有理数值，公式有效. 公式 (2) 和 (3) 叫作**卡尔达诺公式**(1545 年), 对此作出贡献的还有其他文艺复兴时期的意大利数学家 (费罗，塔尔塔利亚). 对四次方程也找到了类似的公式，而寻求五次一般方程根式解的努力延续了几乎 300 年之久，但未能获得成功. 直到 1813 年鲁菲尼 (第一次，粗略地) 和 1827 年阿贝尔 (独立地，完全严格地) 证明了下述定理，n 次一般方程.

$$x^n+a_1x^{n-1}+\cdots+a_n=0$$

当 $n>4$ 时没有根式解.

在这一领域中的本质发现是 1831 年由二十岁的伽罗瓦得到的 (直到 1846 年才为世人所知), 他给出了对任意方程 (例如有理系数方程) 可根式求解的判定法则，而不仅仅局限于一般 n 次方程，对每一个 n 次多项式 (方程), 伽罗瓦给出了一个分裂

域和由这个域的自同构组成的有限集 (基数不超过 $n!$), 现在称之为域的 (或原多项式的)**伽罗瓦群**.

我们把伽罗瓦理论放到 [BAⅢ] 中更详细地讲述. 此处仅完全根据内在的性质区分出一类特殊的 **群**, 称之为 **可解群** . 其结论是, n 次有理系数方程可用根式求解, 当且仅当它对应的伽罗瓦群是可解群. 例如, 设给出五次方程

$$x^5 - ax - 1 = 0,$$

其中 a 是一个整数. 它对应的伽罗瓦群 G_a 以某种复杂的方式依赖于 a; 当 $a = 0$ 时, G_0 是 4 阶循环群 (根据定义, 所有的循环群都是可解的), 从而方程

$$x^5 - 1 = 0$$

是可以根式求解的. 反之, G_1 与 120 阶对称群 S_5 有相同的结构, 而后者在 [BAⅢ] 中证明是一个不可解群. 因而方程

$$x^5 - x - 1 = 0$$

是不能用根式求解的.

我们要注意, 从应用的角度出发, 一个代数方程的解能否用根式明显地表达出来, 并没有本质上的重要意义; 反而是计算根的各种近似方法更实用一些. 但这丝毫无损于伽罗瓦理论的辉煌, 他的成就对后来数学的发展在思想上影响深远. 从那时起, 伽罗瓦奠定了群论的基础. 他建立的分裂域的子域与其伽罗瓦群的子群之间的一一对应到 20 世纪已用新的抽象结构加以充实, 成为数学研究中不可缺少的工具.

2. 多原子分子的状态问题　每一个分子都可以被看作是一个粒子系, 即原子核及环绕原子核的电子. 如果在初始时刻粒子系接近于平衡状态, 则在一定条件下, 粒子系中的粒子总是停留在平衡位置附近, 不会得到较高的速度. 这种类型的运动叫作 *相对不平衡状态的振动*, 并称这样的系统是 **稳定的**.

我们知道, 分子在平衡位置附近的任何小振动都是所谓正常振动的叠加. 在很多情况下, 注意到分子内部的对称性, 可以确定分子的势能及其正常频率. 分子结构的对称性用分子的点群来描述. 这一有限群的不同的实现 (即它的不可约表示) 及其与这些实现相联系的群上的函数 (表示的特征标) 确定了分子振动的参数.

例如水分子 H_2O(见图 1) 对应于克莱因四元群 (两个二阶循环群的直积); 而磷分子 P_4(见图 2) 则形如正四面体, 磷原子分布在顶点上, P_4 对应于对称群 S_4, 其阶为 24. 它的不可约表示在 [BAⅢ] 中给出.

今天分子结构理论的发展没有群论的帮助是难以想象的. 群论在很早以前就被应用到结晶学上. 早在 1891 年, 伟大的俄罗斯结晶学家费得洛夫以及后来德国科学家绍恩费里斯找到了 230 种空间晶体群, 描述了自然界已发现的一切晶体对称. 从那时起, 群论一直被用来研究对称性对晶体物理性质的影响.

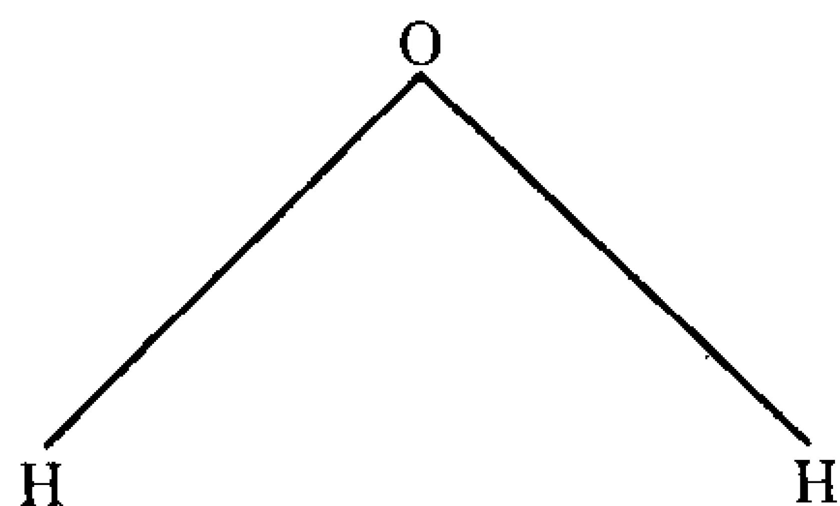


图 1

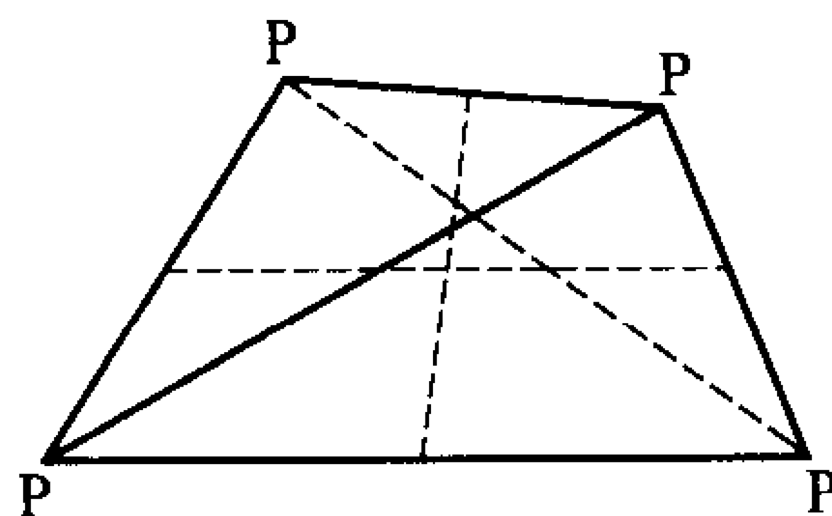


图 2

3. 通信编码问题 在地面上或太空中建立自动通信系统时，被用作基本信息单位的通常是一个有序序列，称之为行 (或字):

$$a = (a_1, a_2, \cdots, a_n),$$

其长度为 $n, a_i = 0$ 或 $a_i = 1$. 因为模 2 的加法和乘法运算在计算机上很好实现，而信号 1,0 本身以电子信号的形式来传送又很方便 (1 和 0 的区分或按照信号时间的相位，或按照信号的有无); 无怪乎 GF(2)(见第 4 章 §3) 被通信专家们用来加工信息. 有时将 a_i 看作其他有限域中的元素也很方便.

为了排除干扰 (大气放电，宇宙噪音等), 这些干扰可能会把 0 变成 1, 把 1 变成 0, 必须使 a 足够长，并采用专门的 **编码** 系统，即从字的全部集合 S 中挑选出由传输行 (字码) 构成的子集 S_0(码), 以便当发生的误差不是太大时，从所收到的变形了的字 a' 恢复到原来的 a. 这样就出现了 **纠错码**.

编码的代数理论近年来发展迅速，给出了许多巧妙的编码方法，该理论主要涉及特殊线性编码: S_0 的选取依赖于特殊长方矩阵的构造和线性方程组的解，它们的系数属于一个给定的有限域，在第 4 章中将给出一个简单的例子.

4. 平板受热问题 带有三个孔的矩形平板 (见图 3) 被当作一种奇妙装置的阀门，以便得到低温. 阀门由正方形方格构成的一个网覆盖着. 位于网的四条边界上的正方形的顶点称为 *边界点*, 而其他的顶点叫作内点. 测量表明，当加热或冷却时，任一内点的温度是它相邻的四个顶点 (内点或边界点) 温度值的算术平均. 我们希望边界点的温度取图 3 所示的值. 这是可能的吗？如果可能，试问内点的温度分布是不是唯一确定的？

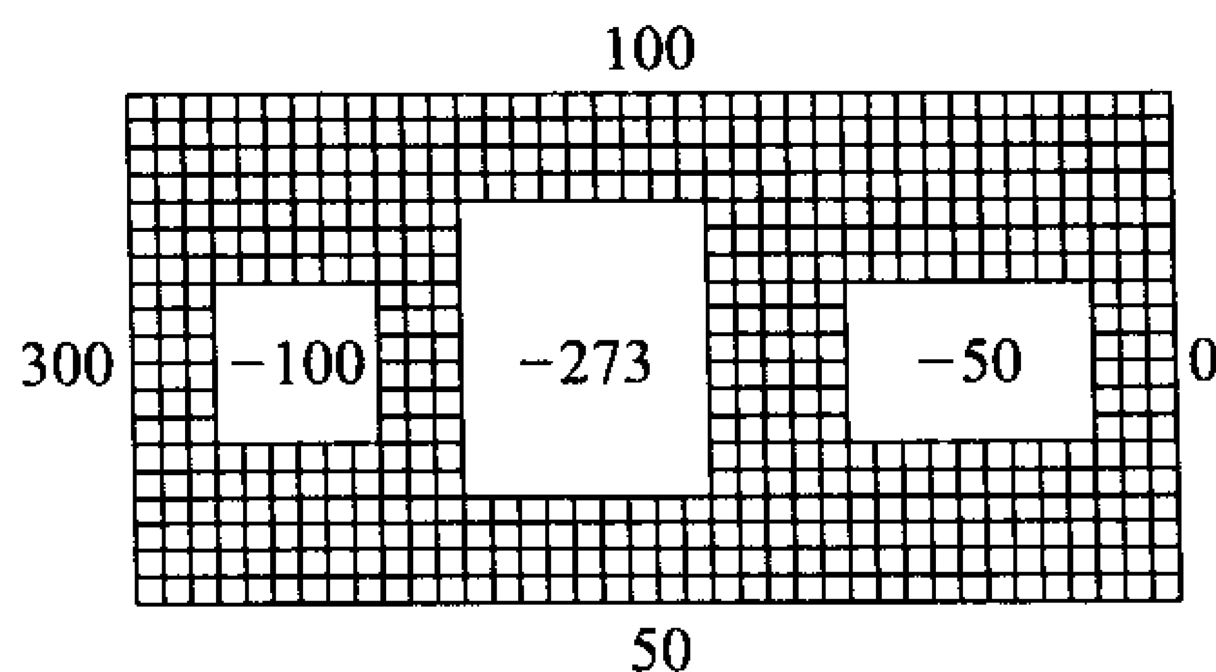


图 3

§3　线性方程组初步

带有实系数 a,b,c,d,e,f 的线性方程 $ax=b$, 以及形如

$$\begin{aligned} ax+by&=e,\\ cx+dy&=f \end{aligned} \tag{1}$$

方程组的求解问题在中学已经学习过了. 我们现在的目的是学会解形如

$$\begin{aligned} a_{11}x_1+a_{12}x_2+\cdots+a_{1n}x_n&=b_1,\\ a_{21}x_1+a_{22}x_2+\cdots+a_{2n}x_n&=b_2,\\ &\cdots\cdots\cdots\cdots\\ a_{m1}x_1+a_{m2}x_2+\cdots+a_{mn}x_n&=b_m \end{aligned} \tag{2}$$

的一般线性代数方程组 (或简称线性方程组). 此处 m,n 是任意正整数. 看起来, 从方程 (1) 过渡到方程 (2) 时纯粹数量上的增长是一件具有本质意义的事情. 形如 (2) 的线性方程组直接出现在几乎所有的数学分支中, 而所谓线性方法, 其最终产物往往是线性方程组的解, 已经成为数学中发展最充分的部分. 简略地说, 形如 (2) 的线性方程组为 19 世纪创立积分方程的理论提供了原型, 而后者在力学和物理学中有着特殊重要的作用. 再如计算机处理的大量实际问题也要归结为线性方程组 (2).

1. 名词　注意到方程组 (2) 的系数使用了非常简明方便的符号: *系数* a_{ij} 表示在第 i 个方程中第 j 个未知数的系数 (读作 "$a-i-j$", 例如 a_{12} 读作 "$a-1-2$", 而不是 "$a-12$"). 数字 b_i 叫作第 i 个方程的 **常数项**. 如果 $b_i=0, i=1,z,\cdots,m$, 称方程组 (2) 为 *齐次的*. 对于任意的一组 $b_i=0, i=1,\cdots,m$, 线性方程组

$$\begin{aligned} a_{11}x_1+a_{12}x_2+\cdots+a_{1n}x_n&=0,\\ a_{21}x_1+a_{22}x_2+\cdots+a_{2n}x_n&=0,\\ &\cdots\cdots\cdots\cdots\\ a_{m1}x_1+a_{m2}x_2+\cdots+a_{mn}x_n&=0 \end{aligned} \tag{2^0}$$

叫作与方程组 (2) 相对应的**齐次方程组**, 或方程组 (2) 的 **诱导组**, 未知数的系数可以排成一个长方形的表

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n}\\ a_{21} & a_{22} & \cdots & a_{2n}\\ \cdots & \cdots & \cdots & \cdots\\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix} \tag{3}$$

叫作一个 $m\times n$ **矩阵**(如果 $m=n$, 则称为 n 阶 **方阵**), 并可简记为 (a_{ij}) 或用字母 A

表示. 自然地 $(a_{i1}, a_{i2}, \cdots, a_{in})$ 叫作矩阵 (3) 的第 i行, 而第 j列

$$\begin{pmatrix} a_{1j} \\ a_{2j} \\ \vdots \\ a_{mj} \end{pmatrix}$$

今后将表示成用方括号括起来的行 $[a_{1j}, a_{2j}, \cdots a_{mj}]$ 以便节省地方. 当矩阵是方阵时, 我们还可以谈它的由元素 $a_{11}, a_{22}, \cdots, a_{nn}$ 组成的 **主对角线**. 除主对角线外, 其他所有元素都等于零的方阵 (a_{ij}), 叫作 **对角矩阵**, 有时记作

$$\mathrm{diag}(a_{11}, a_{22}, \cdots a_{nn}),$$

当 $a_{11} = a_{22} = \cdots = a_{nn} = a$ 时, 称之为 **纯量** 矩阵 , 记作 $\mathrm{diag}_n(a)$. 矩阵 diag_n (1) 叫作 **单位** 矩阵 , 通常记作 E_n, 当矩阵的阶数确定时可简记作 E.

与矩阵 (3) 同时, 我们也考虑方程组 (2) 的 **增广** 矩阵 $(a_{ij}|b_i)$ 它是由矩阵 (3) 增添常数项的列 $[b_1, b_2, \cdots, b_m]$ 得到的; 为清楚起见, 用竖线将该列与其他列分开.

如果用数字 x_i^0 代替未知数 x_i 时, 方程组 (2) 中的每一个方程都变成了恒等式, 则称 n 个数 $x_1^0, x_2^0, \cdots, x_n^0$ 的有序组为方程组 (2) 的一个 **解**, 而 x_i^0 称为解的第 i 个分量 . 这时也称有序组 $x_1^0, x_2^0, \cdots, x_n^0$ 满足 (2) 的每一个方程. 没有任何解的方程组叫作 **不相容的**. 有解的方程组叫作 **相容的**, 如果只有唯一解, 就叫作 **确定的**. 解的个数多于一个的方程组叫作 **不定的**. 一个给定的方程组是否相容, 如果相容, 它的所有的解是什么样的, 这就是我们当前应该回答的问题.

再来看 §2 的第四个问题. 我们给薄板内部的点以任意顺序从 1 到 416 编号 (即图 3 所示的内点总数), 再添加 204 个边界点的号码, 并将需要按照已知规则计算的温度 t_i 放到序号 i 的内点, 编成 416 个相关的式子:

$$t_e = \frac{t_a + t_b + t_c + t_d}{4}.$$

比如说 $a, b, c \leqslant 416, d > 416$. 这时, 关系式可以写成线性方程的形式

$$-t_a - t_b - t_c + 4t_e = t_d.$$

右边的 $t_d = -273, -100, -50, 0, 50, 100, 300$(可能有其他的不同版本). 这些方程构成了一个形如 (2) 的线性方程组, 其中 $n = m = 416$. 未知数 t_i 的系数等于 0(在绝大多数情况下),-1 或 4. 这个方程组是否相容和确定呢?

我们得到了一个定性问题在数学上的准确的定量表达式. 存在性和唯一性问题在由研究物理现象引出的许多数学分支中都是非常典型的问题.

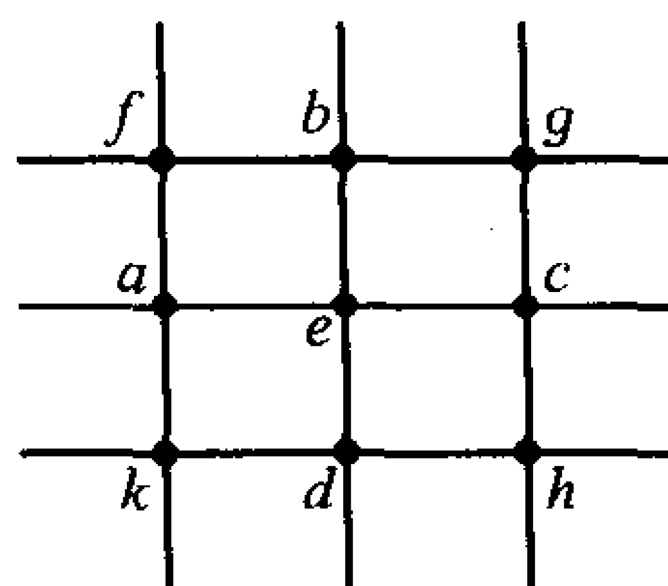


图 4

2. 线性方程组的等价 假设我们还有一个与方程组 (2) 未知数个数与方程个数相同的线性方程组

$$\begin{aligned} a'_{11}x_1 + a'_{12}x_2 + \cdots + a'_{1n}x_n &= b'_1, \\ a'_{21}x_1 + a'_{22}x_2 + \cdots + a'_{2n}x_n &= b'_2, \\ &\cdots\cdots \\ a'_{m1}x_1 + a'_{m2}x_2 + \cdots + a'_{mn}x_n &= b'_m. \end{aligned} \tag{2'}$$

如果方程组 (2) 中除第 i, k 个之外的所有的方程保持不动，而第 i, k 个方程交换位置，则称 (2′) 是由 (2) 经过 (I)**型初等变换** 得到的. 如果 (2) 中除第 i 个之外的所有方程保持不变，而第 i 个方程变为

$$(a_{i1} + ca_{k1})x_1 + \cdots + (a_{in} + ca_{kn})x_n = b_i + cb_k \tag{*}$$

(即 $a'_{ij} = a_{ij} + ca_{kj}, b'_i = b_i + cb_k$), 此处 c 是任意常数，则称方程组 (2′) 是由 (2) 经过 (Ⅱ)**型初等变换** 得到的.

如果两个线性方程组 (2) 和 (2′) 同时是不相容的，或者同时是相容的，且有相同的解，则称 (2) 与 (2′)**等价**. 两个等价的方程组 (a) 和 (b) 记作： $(a) \sim (b)$, 我们注意到， $(a) \sim (a)$,$(a) \sim (b)$ 意味着 $(b) \sim (a)$, 而从 $(a) \sim (b), (b) \sim (c)$ 可推出 $(a) \sim (c)$.

下述论断给出了等价性的一个充分条件.

定理 1 如果一个线性方程组是由另一个线性方程组经过有限多次初等变换得到的，则这两个方程组等价.

证明 只要证明当方程组 (2′) 由方程组 (2) 经一次初等变换得到， (2) 与 (2′) 等价就可以了.

注意到方程 (2) 也是由方程 (2′) 经一个初等变换得到的，因为这些变换是可逆的. 事实上，在情况 (I), 再一次交换第 i, k 个方程的位置，我们就回到了原来的方程组；类似地，在情况 (II), 将第 k 个方程乘以 $(-c)$ 加到 (2′) 中的第 i 个方程上去，我们就得到了 (2) 中的第 i 个方程.

现在我们来证明方程组 (2) 的任意解 $(x_1^0, \cdots, x_n^0)$ 也是 (2′) 的解. 如果施行的初等变换是 (I) 型的，方程自身没有改变 (改变的仅仅是它们的次序). 所以在变换前满足方程的数组 $x_1^0, x_2^0, \cdots, x_n^0$ 在变换后仍满足方程. 在 (Ⅱ) 型初等变换的情况

下，除第 i 个之外的所有方程都没有改变，所以原来方程组的解 $(x_1^0, x_2^0, \cdots, x_n^0)$ 满足这些方程. 至于第 i 个方程，它变成了 $(*)$ 的形式. 因为我们的解满足 (2) 的第 i 和第 k 个方程，所以

$$\begin{aligned} a_{i1}x_1^0 + \cdots + a_{in}x_n^0 &= b_i, \\ a_{k1}x_1^0 + \cdots + a_{kn}x_n^0 &= b_k. \end{aligned}$$

用 c 乘第二个恒等式的两端，并加到第一个恒等式上，我们就得到了形如 $(*)$ 的恒等式，此处 $x_i = x_i^0$.

前面谈到的初等变换的可逆性可以用来证明，反过来，方程组 $(2')$ 的任意解也是 (2) 的解.

最后要说明的是，一个方程组的不相容性意味着另一个的不相容 (通过反证法来证). □

3. 化为阶梯型 通过施行一系列的初等变换，可以将给定的方程组转化为较简单的形式.

首先指出，在系数 a_{i1} 当中至少有一个不等于 0. 否则谈未知数 x_1 就没有意义了. 如果 $a_{11} = 0, a_{j1} \neq 0$, 交换第 1 个方程与第 j 个方程的位置， (用 (I) 型初等变换). 现在第一个方程中第一个未知数的系数非 0. 将它记作 a'_{11}. 从第 i 个方程的两端 $(i = 2, 3, \cdots, m)$ 减去新方程组中第一个方程的两端乘以系数 c_i, 使得减完后 x_1 的系数变为 0(做 $m-1$ 次 (II) 型初等变换). 显然为此必须取 $c_i = a_{21}/a'_{11}$. 结果我们就得到了一个方程组， x_1 只出现在该组的第一个方程中. 这时也可能发生如下情况，即第二个未知数在标号 $i > 1$ 的所有方程中也不出现. 设 x_k 是出现在第一个方程以外的任意一个方程中脚标最小的未知数. 我们得到方程组

$$\begin{array}{llll} a'_{11}x_1 + & & \cdots & +a'_{1n}x_n = b'_1, \\ & a'_{2k}x_k + & \cdots & +a'_{2n}x_n = b'_2, \\ & & \cdots\cdots\cdots\cdots & \\ & & a'_{mk}x_k + \cdots & +a'_{mn}x_n = b'_m, \\ & & & k > 1, a'_{11} \neq 0. \end{array}$$

抛开第一个方程，对所有余下的方程运用上述推理. 经过一系列初等变换，原方程组变成下述形式.

$$\begin{array}{lllll} a''_{11}x_1 + & & & \cdots & +a''_{1n}x_n = b''_1, \\ & a''_{2k}x_k + & & \cdots & +a''_{2n}x_n = b''_2, \\ & & a''_{3l}x_l + & \cdots & +a''_{3n}x_n = b''_3, \\ & & & \cdots\cdots\cdots\cdots & \\ & & & a''_{ml}x_l + \cdots & +a''_{mn}x_n = b''_m, \\ & & & & l > k > 1, a''_{11} \neq 0, a''_{2k} \neq 0. \end{array}$$

因为第一个方程未被涉及，此处自然有 $a''_{1j} = a'_{1j}, b''_1 = b'_1$. 只要还有可能，我们就运用这一过程. 显然，如果在所得方程中头一个未知数 (设脚标为 s) 及其后面直到脚标为 n 的所有未知数的系数都等于 0, 我们就不得不中止这一过程. 这时，方程组 (2) 变为

$$
\begin{aligned}
\bar{a}_{11}x_1 + \quad & \cdots + \bar{a}_{1n}x_n = \bar{b}_1, \\
\bar{a}_{2k}x_k + \quad & \cdots + \bar{a}_{2n}x_n = \bar{b}_2, \\
\bar{a}_{3l}x_l + \quad & \cdots + \bar{a}_{3n}x_n = \bar{b}_3, \\
& \cdots\cdots\cdots \\
\bar{a}_{rs}x_s + \quad & \cdots + \bar{a}_{rn}x_n = \bar{b}_r, \\
& 0 = \bar{b}_{r+1}, \\
& \cdots\cdots\cdots \\
& 0 = \bar{b}_m,
\end{aligned}
\tag{4}
$$

此处 $\bar{a}_{11}\bar{a}_{2k}\bar{a}_{3l}\cdots\bar{a}_{rs} \neq 0, 1 < k < l < \cdots < s$. 如果 $r = m$, 则方程组 (4) 中形如 $0 = \bar{b}_i$ 的方程不会出现. 方程组 (4) 叫作 **阶梯形的**.

这一术语不是唯一通用的，方程组 (4) 有时被称为 **梯形的** 或 **拟三角形的**, 它们都没有本质上的区别.

定理 2 *任意线性方程组都等价于一个 阶梯形方程组 .*

证明可直接由上述推导得到.

有时不把初等变换用于线性方程组，而用于它的增广矩阵 $(a_{ij}|b_i)$. 与定理 2 的证明相同，我们有

定理 2′ *任意矩阵都可以用初等变换化成阶梯形.*

4. 对阶梯形线性方程组的研究 根据定理 1 和定理 2, 相容性和确定性问题只要对阶梯形方程组 (4) 进行研究就可以了.

我们从相容性问题入手. 如果方程组 (4) 包含一个形如 $0 = \bar{b}_t$ 的方程，且 $\bar{b}_t \neq 0$, 则方程组显然是不相容的，因为当未知数取任何值时，等式 $0 = \bar{b}_t$ 都不能成立. 我们来证明，如果方程组 (4) 不包含这种方程，则方程组是相容的.

于是当 $t > r$ 时，令 $\bar{b}_t = 0$, 我们称第 1, 第 2,$\cdots$ 第 r 个方程开头的未知数 $x_1, x_k, x_l, \cdots, x_s$ 为 **主未知数**, 其余的未知数 (如果它们存在的话), 为 **自由变量**. 根据定义，主未知数共有 r 个.

取定自由变量的任意一组值，并代入方程组 (4). 则关于 x_s 的第 r 个方程形如 $ax_s = b$, 其中 $a = \bar{a}_{rs} \neq 0$ 方程有唯一解. 将得到的解 $x_s = x_s^0$ 代入前 $r-1$ 个方程，并在方程组 (4) 中按照自下而上的顺序求解，我们看到，主未知数的值由自由变量的任意一组给定的值唯一确定.

这就证明了

定理 3 *一个线性方程组具有相容性的充分必要条件是，将它转化为阶梯形方程组后，不包含形如 $0 = \bar{b}_t$, 且 $\bar{b}_t \neq 0$ 的方程. 如果这一条件成立，自由变量可以取*

任意值；而主未知数 (在自由变量的任意一组定值之下) 由方程组唯一确定.

现在我们来搞清楚，一个方程组在相容性条件成立的情况下，何时是确定的. 如果方程组 (4) 有自由变量，则方程组显然是不确定的：我们可以给自由变量以任意值，并通过它们来表示主未知数 (定理 3). 如果自由变量不存在，即所有的未知数都是主未知数，则根据定理 3, 主未知数的值由方程组唯一确定，所以方程组是确定的.

注意到没有自由变量等价于条件 $r = n$.

我们证明了下述论断.

定理 4 一个相容的线性方程组 (2) 是确定的，当且仅当由它得到的阶梯形方程组 (4) 满足条件 $r = n$. □

当 $m = n$, 则线性方程组转化为阶梯形时也可以写成如下 (**三角形式**):

$$\begin{aligned} \overline{a}_{11}x_1 + \overline{a}_{12}x_2 + \cdots + \overline{a}_{1n}x_n &= \overline{b}_1, \\ \overline{a}_{22}x_2 + \cdots + \overline{a}_{2n}x_n &= \overline{b}_2, \\ \cdots\cdots\cdots\cdots \\ \overline{a}_{nn}x_n &= \overline{b}_n, \end{aligned} \tag{5}$$

如果我们不在意对任意 i, 是否有 $\overline{a}_{ii} \neq 0$. 事实上，记法 (5) 仅仅表明，方程组中的第 k 个方程不包含未知数 x_i, 其中 $i < k$, 而阶梯形方程组显然满足这一条件.

设 $(\overline{a}_{ij})$ 是一个矩阵，如果当 $i > j$ 时，元素 $a_{ij} = 0$, 则称矩阵为 **上三角** 矩阵 . 类似地可定义 **下三角** 矩阵 .

从定理 3 和公式 (4) 引出

推论 1 线性方程组 (2) 当 $m = n$ 时是相容且确定的，当且仅当将它化为阶梯形后，所得的线性方程组 (5) 满足条件 $\overline{a}_{11}\overline{a}_{22}\cdots\overline{a}_{nn} \neq 0$. □

注意到一个事实, 即这一条件不依赖于方程组中方程的右半部分. 所以当 $m = n$ 时，方程组 (2) 是相容且确定的，当且仅当与之对应的齐次方程组 (2^0) 是相容且确定的. 但是一个齐次方程组永远相容：它至少有一个零解

$$x_1^0 = 0, \ \cdots, \ x_n^0 = 0.$$

条件 $\overline{a}_{11}\overline{a}_{22}\cdots\overline{a}_{nn} \neq 0$ 意味着，齐次方程组仅有零解. 我们得到了推论 1 的另一种形式，它与方程组的阶梯形无关.

推论 1′ 线性方程组 (2) 在 $m = n$ 的情况下是相容的且确定的，当且仅当与之对应的齐次线性方程组 (2^0) 只有零解. □

$n > m$ 的情况值得特别的关注.

推论 2 当 $n > m$ 时，相容的方程组 (2) 是不定的. 特别地，齐次方程组当 $n > m$ 时永远有非零解.

证明 事实上，因为方程组 (4) 的方程个数不会多于方程组 (2)(去掉左右两边

恒等于零的方程), 在任何情况下都有 $r \leqslant m$. 所以不等式 $n > m$ 意味着 $n > r$, 根据定理 4 方程组 (2) 是不定的. 最后要指出，齐次方程组的不定性，等价于非零解的存在性.

我们得到的结果反映在下表中.

	线性方程组的类型			
	一般	齐次	$n > m$ 非齐次	$n > m$ 齐次
解的个数	0 1 ∞	1 ∞	0 ∞	∞

5. 评注和例子 上述解线性方程组的方法叫作 **高斯法** 或 **逐次消元法**. 当 n 不大时这种方法是非常方便的，并且适用于计算机实现. 可是由于种种原因，其他的一些解法，例如迭代法往往更切合实际. 当系数给定时，寻找具有确定精确度的解就属于这种情况. 但是在理论研究中，最重要的问题是得到线性方程组相容性或确定性条件的表述，并寻求用系数和常数项表示解的一般公式，而不必将方程组化为阶梯形. 推论 1′ 就在某种程度上符合这一点.

例 1 重新回到 §2 的薄板受热问题. 正如本节第一段所示，引起我们兴趣的这一问题变成了一个非常具体的线性方程组 (为确定起见，将其记作 HP) 的求解问题，该方程组含有非常多的未知数 t_i. 按照推论 1′ 中陈述的判别法，我们来研究对应于 HP 的齐次线性方程组 (HHP). 换言之，薄板所有的边界点的温度现在取零. 设 e 是一个内顶点的脚标，该点的温度有 极大 值 $|t_e|$. 这时条件

$$t_e = \frac{t_a + t_b + t_c + t_d}{4}$$

意味着 $|t_e| = |t_a| = |t_b| = |t_c| = |t_d|$. 在没有达到温度为 0 的边界点之前，我们沿着点阵中由一个内点给出的四个方向中的任意一个方向移动一步，就会看到所有的点均取值 $|t_i| = |t_e|$. 这就意味着 $|t_e| = 0$, 所以对任意的脚标 $i, t_i = 0$. 因而方程组 HHP 仅有零解，故 HP 是一个相容的且确定的线性方程组. 这样最初提到的薄板受热问题本身也就解决了.

例 2 给出线性方程组

$$\begin{aligned}
x_1 \qquad\qquad\qquad\qquad &= 1,\\
x_2 \qquad\qquad\qquad &= 1,\\
-x_1 - x_2 + x_3 \qquad\qquad &= 0,\\
\cdots\cdots\cdots\cdots &\\
-x_{n-2} - x_{n-1} + x_n &= 0.
\end{aligned}$$

这显然是一个相容的且确定的方程组, 它已经成为阶梯形 (三角形) 了. 只不过求解时不是自下而上, 而是自上而下. 按照定义, 它的解是前 n 个 **斐波那契数** $f_1, f_2, \cdots, f_n$.

这些数与植物现象中的叶序数 (叶子在茎上的排列) 有关. 与其孤立地求解 $n=1000$ 或任意给定的 n. 不如得到对第 n 个斐波那契数的一般表达式 (解析 公式). 你可能会反对说, 我们有足够的耐心, 就可以根据这些数的归纳定义给出 f_{1000}. 但这不是解决数学问题的根本办法. 我们将在第二章和第三章中给出 f_n 的两个表达式, 尽管这个具体问题可以用更直接的办法来解.

注记 1 有时不必化阶梯形就可以更方便地求出线性方程组的解. 特别是当线性方程组的矩阵包含很多零时. 此时简短的实际解法取代了冗长的解释.

注记 2 当我们用高斯法解 n 元 n 个方程的线性方程组时经过多少步必要的算术运算 Γ_n 可以完成求解? 这不是一个等闲的问题, 因为在通常情况下, 当我们对大数 n 使用计算机时, 应当对求解问题所需的机时进行预先估计.

因为两数相乘要比相加工作量大, 所以建议只计算做乘法的次数, 自然也包括除法, 以后简称运算. 不失一般性, 可以假定线性方程组有唯一解, 即所有的未知数都是主未知数. 暂且忽略方程的右边. 为了从第 i 个方程 $(i>1)$ 消去未知数 x_1 需准备好数 $l_i=a_{i1}/a_{11}$(做一次除法), 还要算出 $n-1$ 个乘积 $l_ia_{ij}, j=2,3,\cdots n$, 即共需要 n 次运算. 按照我们的约定, 忽略从第 i 个方程减去第一个方程的 l_i 倍的过程. 因为 $i=2,3,\cdots,n$, 那么为了消去 x_1, 需要 $n(n-1)$ 次运算. 第二步, 我们对得到的 $(n-1)$ 阶方程组需要 $(n-1)(n-2)$ 次运算, 第三步相应地为 $(n-2)(n-3)$ 等等. 为了将方程组的左边化为如同公式 (5) 的三角形式, 总运算次数为和式

$$\Gamma(n)=n(n-1)+(n-1)(n-2)+\cdots+1(1-1).$$

不难验证 (自己证明或者参看 §7),

$$\Gamma(n)=\frac{n^3-n}{3}.$$

找到解的分量 $x_n^0, x_{n-1}^0,\cdots,x_1^0$(按方程组 (5) 自下而上运作), 共需要

$$1+2+3+\cdots+n=\frac{n(n+1)}{2}$$

次运算, 当 n 较大时, 并不引起对运算次数总和的本质影响. 于是, 高斯算法相当准确的运算次数是 $\Gamma_n=n^3/3$.

1969 年, 施特拉辛研究出一种方法, (详见 [BAII]), 仅需

$$S_n=C\cdot n^{\log_2 7}\approx C\cdot n^{2.81}$$

次运算, 当 n 非常大时, 可以节省大量运算, 诚然, 做到这一点是由于增加了加法运算的次数. 但 S_n 中的常数 C 特别大, 而实现它的程序在逻辑上又很复杂, 因而这里所谈的节省仍停留在理论上的计划.

我们所了解的两种方法是典型的数学算法, 适用于大量问题的解决. 稍后我们会看到算法的其他例子. 它们的作用在我们这个全盘计算机化的时代是非常巨大的. 这时重要的不但是算法本身, 还有对计算复杂性的估计.

§4　低阶行列式

在介绍高斯方法时, 我们没有过多地关注主未知数系数的值. 那时着重关注于这些系数是非零的. 现在我们进入消元法的精确步骤, 尽管只是解低阶方形线性方程组. 这样做将为我们提供一些思考的案例, 以及在第三章给出的构造一般行列式理论的原始材料.

如 §3 所示, 考虑带有两个未知数的两个方程

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 = b_1, \\ a_{21}x_1 + a_{22}x_2 = b_2, \end{aligned} \tag{1}$$

并试图寻找解的分量 x_1^0, x_2^0 的一般公式.

矩阵 $\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$ 的 **行列式** 是一个表达式 $a_{11}a_{22} - a_{21}a_{12}$, 记作

$$\begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix}.$$

这样二阶方阵本身对应于一个数

$$\begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} = a_{11}a_{22} - a_{21}a_{12}. \tag{2}$$

如果我们希望从方程组 (1) 中消去 x_2, 则将第一个方程乘以 a_{22}, 第二个方程乘以 $(-a_{12})$, 然后相加, 得到

$$\begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} x_1 = b_1a_{22} - b_2a_{12}.$$

可以看到, 方程的右边恰为矩阵 $\begin{pmatrix} b_1 & a_{12} \\ b_2 & a_{22} \end{pmatrix}$ 的行列式. 设 $\begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} \neq 0$. 于是我们有

$$x_1 = \frac{\begin{vmatrix} b_1 & a_{12} \\ b_2 & a_{22} \end{vmatrix}}{\begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix}}, \qquad x_2 = \frac{\begin{vmatrix} a_{11} & b_1 \\ a_{12} & b_2 \end{vmatrix}}{\begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix}}. \tag{3}$$

有了含两个未知数，两个方程的线性方程组的求解公式，我们也能够解某些其他的方程组了 (解方程组 —— 意味着找出它们的解). 例如，我们考察含三个未知数，两个齐次方程的线性方程组

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + a_{13}x_3 &= 0, \\ a_{21}x_1 + a_{22}x_2 + a_{23}x_3 &= 0. \end{aligned} \tag{4}$$

我们的兴趣在于找出这个方程组的非零解, 即至少有一个 $x_i \neq 0$ 的解. 例如设 $x_3 \neq 0$. 用 x_3 去除方程的两端，并设 $y_1 = -\dfrac{x_1}{x_3}, y_2 = -\dfrac{x_2}{x_3}$, 将方程组 (4) 写成 (1) 的形式

$$\begin{aligned} a_{11}y_1 + a_{12}y_2 &= a_{13}, \\ a_{21}y_1 + a_{22}y_2 &= a_{23}. \end{aligned}$$

当行列式 $\begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} \neq 0$ 时，公式 (3) 给出

$$y_1 = -\frac{x_1}{x_3} = \frac{\begin{vmatrix} a_{13} & a_{12} \\ a_{23} & a_{22} \end{vmatrix}}{\begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix}}, y_2 = -\frac{x_2}{x_3} = \frac{\begin{vmatrix} a_{11} & a_{13} \\ a_{21} & a_{23} \end{vmatrix}}{\begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix}}.$$

毫不奇怪, 我们从方程组 (4) 出发得不到 x_1, x_2, x_3 本身, 而只能得到它们的比: 由方程组的齐次性易见，如果 (x_1^0, x_2^0, x_3^0) 是解，且 c 是任意常数，则 (cx_1^0, cx_2^0, cx_3^0) 也是解. 所以我们可以从

$$x_1 = -\begin{vmatrix} a_{13} & a_{12} \\ a_{23} & a_{22} \end{vmatrix}, x_2 = -\begin{vmatrix} a_{11} & a_{13} \\ a_{21} & a_{23} \end{vmatrix}, x_3 = \begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} \tag{5}$$

入手，方程组的任意解均可由对所有的 x_i 乘以某个常数 c 得到. 为了具有更对称的答案，从公式 (2) 直接导出

$$\begin{vmatrix} a & b \\ c & d \end{vmatrix} = -\begin{vmatrix} b & a \\ d & c \end{vmatrix}.$$

因而 (5) 能够写成下述形式:

$$x_1 = \begin{vmatrix} a_{12} & a_{13} \\ a_{22} & a_{23} \end{vmatrix}, \quad x_2 = -\begin{vmatrix} a_{11} & a_{13} \\ a_{21} & a_{23} \end{vmatrix}, \quad x_3 = \begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix}. \tag{6}$$

这些公式是在 $\begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} \neq 0$ 的假设下推导出来的. 不难验证，只要公式 (6) 中的任意一个行列式不等于零，所给的结论就是正确的. 如果三个行列式都等于零，尽

管公式 (6) 给出了一个零解，但我们不能断定所有的解都可以用它乘以一个常数得到 (例如考虑由两个相同的方程 $x_1+x_2+x_3=0$ 组成的方程组).

现在转到含三个未知数三个方程的方程组

$$
\begin{aligned}
a_{11}x_1+a_{12}x_2+a_{13}x_3&=0,\\
a_{21}x_1+a_{22}x_2+a_{23}x_3&=0,\\
a_{31}x_1+a_{32}x_2+a_{33}x_3&=0.
\end{aligned}
$$

我们希望从这个方程组中消去 x_2 和 x_3, 以便得到 x_1 的值. 为此将第一个方程乘以 c_1, 第二个方程乘以 c_2, 第三个方程乘以 c_3, 并将所得结果相加. 然后选取 c_1,c_2,c_3, 使得在所得方程中含 x_2 及 x_3 的项为零. 令 x_2 和 x_3 的系数等于零，我们就得到了关于 c_1,c_2,c_3 的方程

$$
\begin{aligned}
a_{12}c_1+a_{22}c_2+a_{32}c_3&=0,\\
a_{13}c_1+a_{23}c_2+a_{33}c_3&=0,
\end{aligned}
$$

与方程组 (4) 属同一类型. 因而可取

$$
c_1=\begin{vmatrix} a_{22} & a_{32}\\ a_{23} & a_{33}\end{vmatrix}, c_2=-\begin{vmatrix} a_{12} & a_{32}\\ a_{13} & a_{33}\end{vmatrix}, c_3=\begin{vmatrix} a_{12} & a_{22}\\ a_{13} & a_{23}\end{vmatrix}.
$$

经过显然的替换之后，我们得到了关于 x_1 的表达式

$$
\begin{aligned}
&\left(a_{11}\begin{vmatrix} a_{22} & a_{23}\\ a_{32} & a_{33}\end{vmatrix}-a_{21}\begin{vmatrix} a_{12} & a_{13}\\ a_{32} & a_{33}\end{vmatrix}+a_{31}\begin{vmatrix} a_{12} & a_{13}\\ a_{22} & a_{23}\end{vmatrix}\right)x_1\\
&=b_1\begin{vmatrix} a_{22} & a_{23}\\ a_{32} & a_{33}\end{vmatrix}-b_2\begin{vmatrix} a_{12} & a_{13}\\ a_{32} & a_{33}\end{vmatrix}+b_3\begin{vmatrix} a_{12} & a_{13}\\ a_{22} & a_{23}\end{vmatrix}.
\end{aligned}
\tag{7}
$$

式中 x_1 的系数叫作矩阵

$$
\begin{pmatrix} a_{11} & a_{12} & a_{13}\\ a_{21} & a_{22} & a_{23}\\ a_{31} & a_{32} & a_{33}\end{pmatrix}
$$

的行列式，并记作

$$
\begin{vmatrix} a_{11} & a_{12} & a_{13}\\ a_{21} & a_{22} & a_{23}\\ a_{31} & a_{32} & a_{33}\end{vmatrix}.
$$

这样我们就借助于二阶行列式给出了三阶行列式的表达式

$$
\begin{aligned}
\begin{vmatrix} a_{11} & a_{12} & a_{13}\\ a_{21} & a_{22} & a_{23}\\ a_{31} & a_{32} & a_{33}\end{vmatrix}&=a_{11}\begin{vmatrix} a_{22} & a_{23}\\ a_{32} & a_{33}\end{vmatrix}-a_{21}\begin{vmatrix} a_{12} & a_{13}\\ a_{32} & a_{33}\end{vmatrix}+a_{31}\begin{vmatrix} a_{12} & a_{13}\\ a_{22} & a_{23}\end{vmatrix}\\
&=a_{11}a_{22}a_{33}+a_{12}a_{23}a_{31}+a_{13}a_{21}a_{32}-a_{11}a_{23}a_{32}-a_{12}a_{21}a_{33}-a_{13}a_{22}a_{31}.
\end{aligned}
\tag{8}
$$

容易发现，等式 (7) 的右边是将 x_1 的系数 a_{11} 换成 b_1,a_{21} 换成 b_2,a_{31} 换成 b_3 得到的．所以 (7) 式可以写成

$$\begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} x_1 = \begin{vmatrix} b_1 & a_{12} & a_{13} \\ b_2 & a_{22} & a_{23} \\ b_3 & a_{32} & a_{33} \end{vmatrix}.$$

设 x_1 的系数不等于零．这时通过对 x_2, x_3 的类似计算，我们可以得到表述 x_1, x_2, x_3 的下述公式

$$x_1 = \frac{\begin{vmatrix} b_1 & a_{12} & a_{13} \\ b_2 & a_{22} & a_{23} \\ b_3 & a_{32} & a_{33} \end{vmatrix}}{\begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix}}, \quad x_2 = \frac{\begin{vmatrix} a_{11} & b_1 & a_{13} \\ a_{21} & b_2 & a_{23} \\ a_{31} & b_3 & a_{33} \end{vmatrix}}{\begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix}}, \quad x_3 = \frac{\begin{vmatrix} a_{11} & a_{12} & b_1 \\ a_{21} & a_{22} & b_2 \\ a_{31} & a_{32} & b_3 \end{vmatrix}}{\begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix}}. \tag{9}$$

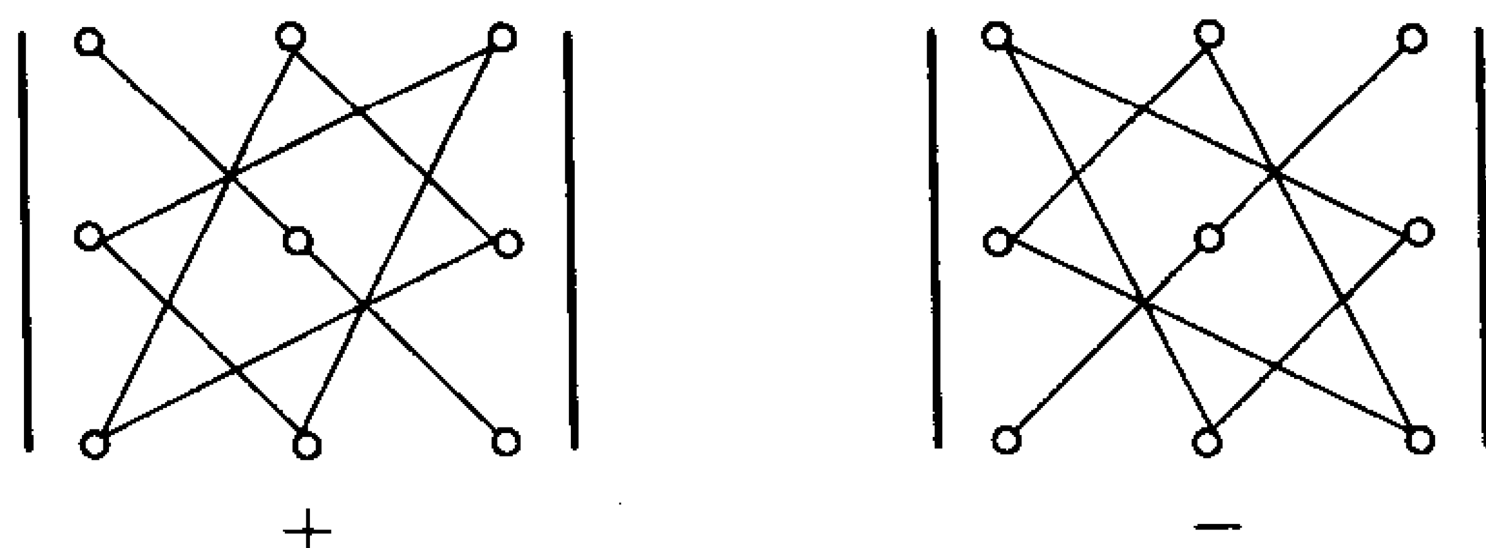
显然，同样的推理适用于四个，五个或更多的方程组成的方程组，只要未知数的个数与方程的个数相同．为此我们必须首先引出一个类似于 (6) 的公式，对含有四个未知数，三个方程的齐次线性方程组求解；然后在含有四个未知数，四个方程的线性方程组中消去 x_2, x_3, x_4，为此用 c_1, c_2, c_3, c_4 分别去乘四个方程并将结果相加．我们从三个齐次方程的方程组中找到 $c_i (i = 1, 2, 3, 4)$ 的值．

这样得到的 x_1 的系数叫作 **四阶行列式**，它可以仿照 (8) 由三阶行列式表出．

经过对 x_2, x_3, x_4 的相同论证，我们找到类似于 (9) 的对 x_i 的公式．这一过程可以无限地进行下去．在数学中有广泛应用的数学归纳法原理 (见 §7) 确保我们总会达到目的．

习　　题

1. 如果用下列直观的符号法则来描述三阶行列式展开式中出现的乘积，就容易记住公式 (8) 了．



对四阶行列式可找到类似的法则．

2. 证明在三阶行列式展开式中的六项不可能同时为正.

3. 验证

$$\begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} = \begin{vmatrix} a_{11} & a_{21} & a_{31} \\ a_{12} & a_{22} & a_{32} \\ a_{13} & a_{23} & a_{33} \end{vmatrix}, \quad \begin{vmatrix} 0 & a & b \\ -a & 0 & c \\ -b & -c & 0 \end{vmatrix} = 0.$$

§5 集合与映射

在前两节中，我们遇到了各式各样的元素的集合，也遇到了集合之间的映射．例如给定的线性方程组的解的集合，或使每一个二阶矩阵对应于它的行列式的法则——都是某些形式概念的特例，了解形式概念 (哪怕在直观的层面上) 对今后的学习是非常有益的．

1. 集合 **集合** 指某些对象的总合，这些对象被称为 **元素**．

含有有限个不同元素的集合可以用明确地列出全部元素的办法来描述，通常将这些元素写在花括号内．例如 $\{1,2,4,8\}$——从 1 到 10 之间 2 的方幂的集合．我们总是用某个字母表中的大写字母表示集合，用同一个或另一个字母表中的小写字母表示它的元素．

对于某些特殊重要的集合采用应当遵循的标准化记法．例如字母 $\mathbb{N},\mathbb{Z},\mathbb{Q},\mathbb{R}$ 分别表示正整数 (自然数) 的集合，全体整数的集合，有理数集和实数集．

给定一个集合 S, **包含** 符号 $a \in S$ 表明 a 是 S 的一个元素；反之，写 $a \notin S$.

如果蕴含关系

$$\forall\, x,\ x \in S \Rightarrow x \in T$$

成立，则称 S 是 T 的一个 **子集**, 并记作 $S \subset T$ (S 包含在 T 中)(关于这一记法，请参考 “给读者的建议” 一节).

如果两个集合 S 与 T 有相同的元素，则称它们重合 (或相等), 用符号的形式写成：

$$S = T \Leftrightarrow S \subset T, \quad T \subset S$$

($\Leftrightarrow$ 表示 “当且仅当” 或 “双向蕴含”).

不包含任何元素的集合叫作 **空集**, 记作 $\varnothing$, 根据定义，空集是任意集合的子集．如果 $S \subset T$, 但 $S \neq \varnothing$, 且 $S \neq T$, 则 S 叫作 T 的 **真子集**. 为了区分出子集 $S \subset T$, 常常指明只有 S 中的元素才具有的性质．例如

$$\{n \in \mathbb{Z} | n = 2m, m \in \mathbb{Z}\}$$

是全体偶整数的集合，而

$$\mathbb{N} = \{n \in \mathbb{Z} | n > 0\}$$

是自然数的集合.

两个集合 S 与 T 的 **交集** 是指集合

$$S\cap T=\left\{x\,\middle|\,x\in S\text{ 且 }x\in T\right\},$$

而 **并集** 指集合

$$S\cup T=\left\{x\,\middle|\,x\in S\text{ 或 }x\in T\right\}.$$

交集 $S\cap T$ 可能是空集. 这时称 S 和 T 是 **不相交的集合**. 交和并的运算满足恒等式

$$R\cap(S\cup T)=(R\cap S)\cup(R\cap T),$$
$$R\cup(S\cap T)=(R\cup S)\cap(R\cup T),$$

我们将这些式子的验证留作习题. 图 5 有助于得出简单的论证.

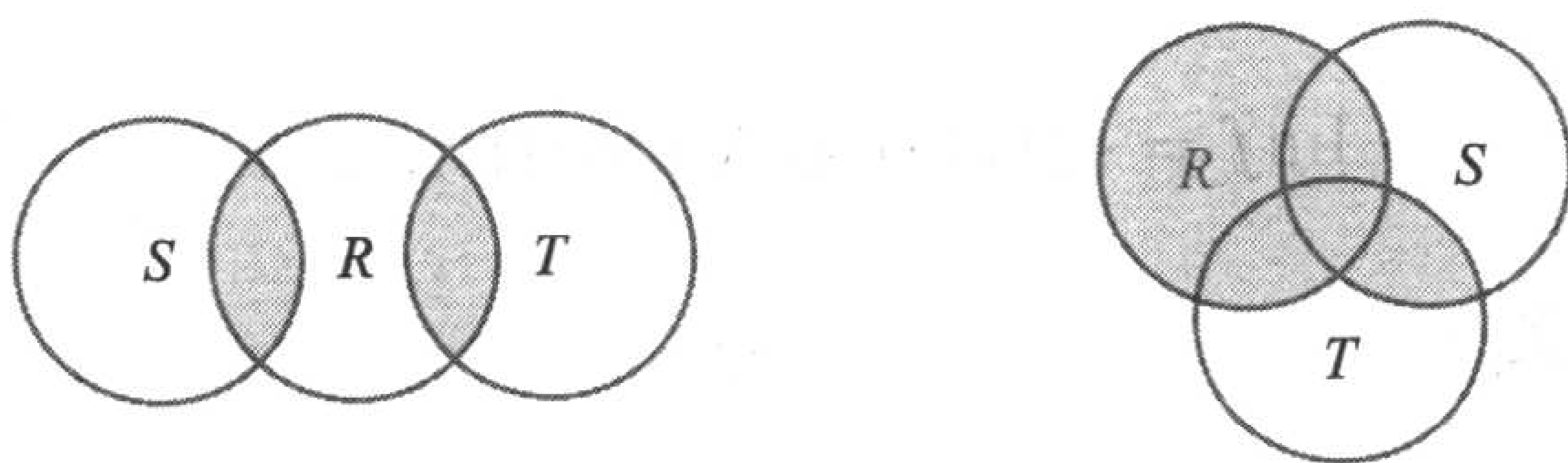


图 5

两个集合 S 与 T 的 **差集**$S\backslash T$ 指属于 S 但不属于 T 的元素的全体. 在这里一般不假设 $T\subset S$, 有时也写 $S-T$ 代替 $S\backslash T$.

如果 T 是 S 的子集, 也称 $S\backslash T$ 为 T 在 S 中的 **补集**. 设 $R=S\backslash T$, 则 $R\cap T=\varnothing$, $R\cup T=S$. 注意集合的运算交、并、补与逻辑连词 "且"、"或"、"非" 之间存在着对应关系.

设 X,Y 是任意两个集合. 任取 $x\in X$, $y\in Y$, 给定顺序的元素对 (x,y), 叫作一个 **有序对**, 这时两个有序对 $(x_1,y_1)=(x_2,y_2)$, 当且仅当 $x_1=x_2$, $y_1=y_2$.

全体有序对 (x,y) 的集合:

$$X\times Y=\{(x,y)|x\in X,y\in Y\}$$

叫作两个集合 X 和 Y 的 **笛卡儿积**.

例如设 $\mathbb{R}$ 是实数集. 这时 **笛卡儿平方** $\mathbb{R}^2=\mathbb{R}\times\mathbb{R}$ 就是在选定了坐标系的平面上点的笛卡儿坐标的集合. 类似地, 可以引出三个集合的笛卡儿积 $X_1\times X_2\times X_3\,(=(X_1\times X_2)\times X_3=X_1\times(X_2\times X_3))$, 以及四个集合的笛卡儿积等等.

当 $X_1=X_2=\cdots=X_k$ 时, 简记作

$$X^k=X\times X\times\cdots\times X$$

并称之为集合 X 的 k 次 笛卡儿方幂. X^k 的元素是长为 k 的序列 (或行)$(x_1,x_2,\cdots,x_k)$.

为了区分集合 $X\times Y$ 和 $X\cup Y$，我们来看 X 和 Y 都具有有限基数 (cardinality) 的情况：

$$|X| = \mathrm{Card}\,X = n,\quad Y = \mathrm{Card}\,Y = m.$$

这时

$$|X\times Y| = n\cdot m,\quad |X\cup Y| = n+m-|X\cap Y|.$$

如果还不清楚，请从头细读有关的定义.

2. 映射 **映射** 或 **函数** 的概念在数学中扮演着中心的角色. 给定两个集合 X 和 Y, 以 X 为 **定义域**, Y 为 **值域** 的映射 f 将每个元素 $x\in X$ 都对应于一个元素 $f(x)\in Y$, $f(x)$ 亦可记作 fx 或 f_x. 当 $X=Y$ 时， f 也叫作集合 X 到自身的一个 **变换**. 用符号表示映射时写作 $f: X\to Y$ 或 $X\xrightarrow{f}Y$.

所有形如 $f(x)$ 的元素的集合叫作映射 f 的像：

$$\mathrm{Im} f = \{f(x)\,|x\in X\} = f(X)\subset Y$$

(Im 取自 image(英文)).

集合

$$f^{-1}(y) = \{x\in X\mid f(x)=y\}$$

叫作元素 $y\in Y$ 的 **原像**. 更一般地：对于 $Y_0\subset Y$, 令

$$f^{-1}(Y_0) = \{x\in X\,|f(x)\in Y_0\} = \bigcup_{y\in Y_0} f^{-1}(y).$$

如果 $y\in Y\backslash\mathrm{Im} f$，则显然有 $f^{-1}(y)=\varnothing$.

设 $f\ X\to Y$ 是一个映射，如果 $\mathrm{Im} f = Y$，则称 f 为 **满射**(surjective(法文)) 或映上的；如果 $x\neq x'$ 意味着 $f(x)\neq f(x')$, 则称 f 为 **单射**(injective(法文)). 最后，如果 $f:\ X\to Y$ 既是满射又是单射，则称 f 为 **双射**(bijective(法文)) 或 **一一映射**.

两个映射相等 $f=g$, 指它们有相同的定义域和值域：

$$X\xrightarrow{f}Y,\quad X\xrightarrow{g}Y,$$

并且 $\forall x\in X, f(x)=g(x)$, 自变量 x, 即元素 $x\in X$ 与其值 $f(x)\in Y$ 的对应通常借助于一个 短箭号表示出来： $x\mapsto f(x)$.

例如设 f_n 是第 n 个斐波那契数 (见 §3). 则对应关系 $n\mapsto f_n$ 定义了一个 $\mathbb{N}\to\mathbb{N}$ 的映射，它既不是满射，也因为 $f_1=f_2$ 显然不是单射. 再如若 $\mathbb{R}_+$ 是正实数的集合，则由同一个规则 $x\mapsto x^2$ 定义的映射

$$f: \mathbb{R}\to\mathbb{R},\qquad g: \mathbb{R}\to\mathbb{R}_+\bigcup\{0\},\qquad h: \mathbb{R}_+\to\mathbb{R}_+$$

是彼此不同的：f 既不满也不单，g 是满射但不是单射，h 是双射．由此看来，确定定义域和值域是定义一个映射 (函数) 的本质部分．

将每一个元素 $x \in X$ 映到自身的映射 $e_x: X \to X$ 叫作 **单位映射**(或 **恒等映射**)．如果 X 是 Y 的子集：$X \subset Y$，有时定义一个专门的 **包含映射** $I: X \to Y$ 是有益的，I 将任意元素 $x \in X$ 映到自身，但将后者看作是在集合 Y 中．映射 $f: X \to Y$ 叫作 **映射** $g: X' \to Y'$ 的 **收缩**(或 **限制**)，如果 $X \subset X', Y \subset Y'$，且 $\forall x \in X$, $f(x) = g(x)$．而 g 叫作映射 f 的 **扩张**．例如嵌入映射 $I: X \to Y$ 是恒等映射 $e_y: Y \to Y$ 的限制．

我们也可以考虑多变元函数．集合 X 的笛卡儿方幂 X^n 的概念为我们提供了定义多变元函数 $f(x_1, \cdots, x_n)$ 的可能性，其中 $x_i \in X, i = 1, \cdots, n$，这个函数就是一般的映射 $f: X^n \to Y$．了解此点是有益处的．

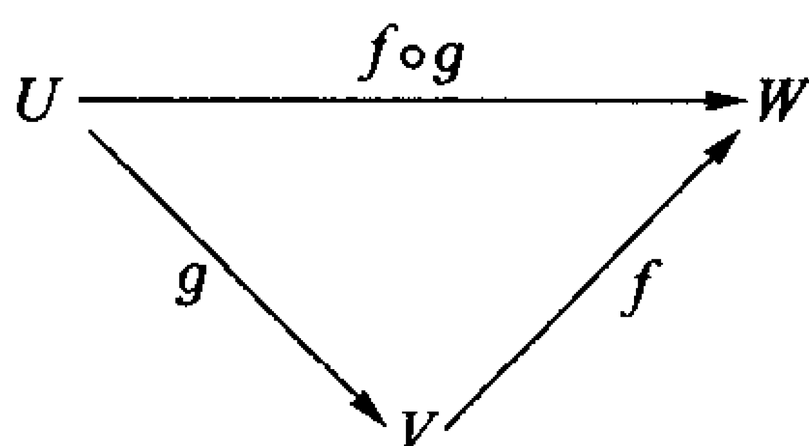
设 $g: U \to V, f: V \to W$ 是两个映射，由法则

$$(f \circ g)(u) = f(g(u))$$

定义的映射

$$f \circ g: U \to W$$

叫作 g 和 f 的 **乘积**(**叠加** 或 **合成**)．用下述 三角图 可以将 $f \circ g$ 直观地描述出来：



我们说这个图形 **可换**(或是 **变换的**)，即从 U 到 W 的结果不依赖于从 $f \circ g$ 直接得到或通过中间阶段 V 得到．注意合成的定义不是对任意映射 f 和 g 都适用的．在上述记法中，它们必须有一个公共的集合 V．但是集合 X 到自身的两个映射的合成永远有意义．

今后我们用简写 fg 代替 $f \circ g$．任取映射 $f: X \to Y$，我们有

$$fe_X = f, \quad e_Y f = f.$$

这一性质的验证是显然的．合成 (乘积) 的一个重要性质表述如下．

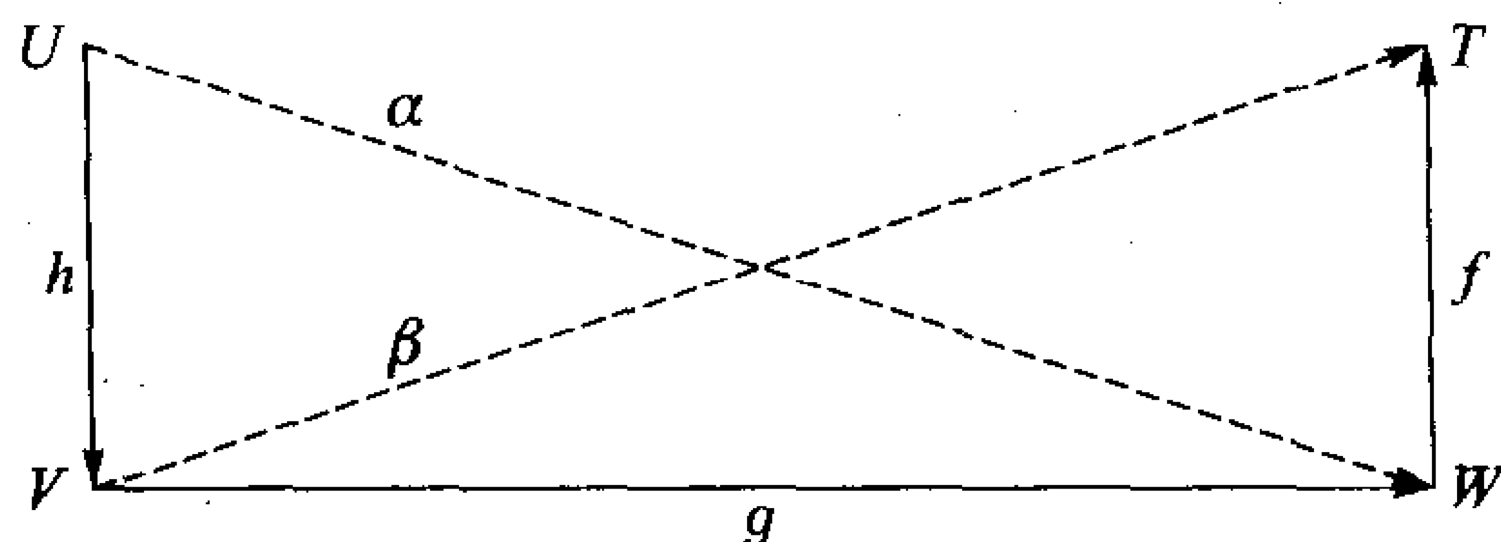
定理 1　映射的合成满足结合律．也就是说，如果

$$h: U \to V, \quad g: V \to W, \quad f: W \to T$$

是三个映射，则

$$f(gh) = (fg)h.$$

证明　直观地讲，所有必要的论证包含在下图中：



此处 $\alpha = gh$, $\beta = fg$. 根据映射相等的定义，需要比较映射 $f(gh)$： $U \to T$ 和 $(fg)h$： $U \to T$ 在任意点 $u \in U$ 的值. 但按照映射合成的定义，我们有

$$(f(gh))(u) = f((gh)(u)) = f(g(h(u))) = (fg)(h(u)) = ((fg)h)(u). \qquad \square$$

一般来说，集合 X 的映射的合成是不交换的，即 $fg \neq gf$. 这很容易从下例中看到，设 $X = \{a, b\}$ 是两个元素的集合，令 $f(a) = b$, $f(b) = a$, $g(a) = a$,$g(b) = a$. 另一个例子：设 f 和 g 都是集合 X 的 **常值映射**, 即 $f(x)$ 和 $g(x)$ 不依赖于 x 的选取. 则 $f \neq g$ 意味着 $fg \neq gf$.

某些映射有 **逆映射**. 设 f： $X \to Y$, g： $Y \to X$ 是两个映射，则合成映射 fg 和 gf 是确定的. 如果 $fg = e_Y$, 那么 f 叫作 g 的 **左逆**, 而 g 叫作 f 的 **右逆**. 当任意顺序的合成都是恒等映射，即：

$$fg = e_Y, \quad gf = e_X \tag{1}$$

时，则称 g 为 f 的 **双边逆**(或简称 **逆**)(而 f 也叫作 g 的逆), 并记作 f^{-1}. 这样, $f(u) = v \Leftrightarrow f^{-1}(v) = u$.

假设还存在着另一个映射 g'： $Y \to X$, 使得

$$fg' = e_Y, \quad g'f = e_X, \tag{1'}$$

则根据等式 (1),(1′) 和定理 1, 我们得到

$$g' = e_X g' = (gf)g' = g(fg') = ge_Y = g.$$

所以 f 的双边逆一旦存在，必定是唯一的. 这也证实了符号 f^{-1} 的含意是明确的.

定理 2 映射 f: $X \to Y$ 有逆，当且仅当 f 是双射.

证明 定理的证明依赖于下述引理，引理自身也是有趣的.

引理 设

$$f: X \to Y, \quad g: Y \to X$$

是任意两个映射，如果 $gf = e_X$, 则 f 是单的，而 g 是满的.

证明 事实上，设 $x, x' \in X$, 且 $f(x) = f(x')$. 则

$$x = e_X(x) = (gf)(x) = g(f(x)) = g(f(x')) = (gf)(x') = e_X(x') = x'.$$

因此 f 是单射. 如果给出 X 的任意元素 x, 则

$$x = e_X(x) = (gf)(x) = g(f(x)),$$

这就证明了 g 是满射. □

回到定理 2, 先设 f 有逆映射 $g = f^{-1}$. 则等式 (1) 和引理给出了 f 的满单性. 换言之, f 是双射. 反过来, 设 f 是一个双射, 则任取 $y \in Y$, 可以求出 唯一 的元素 $x \in X$, 使得 $f(x) = y$. 令 $g(y) = x$, 我们就定义了一个映射 $g: Y \to X$, 且 g 满足性质 (1). 这就意味着 $f^{-1} = g$. □

推论 *从双射 $f: X \to Y$ 得到一个双射 f^{-1}, 且*

$$(f^{-1})^{-1} = f. \tag{2}$$

设 $f: X \to Y$, $h: Y \to Z$ 都是双射, 则合成映射 hf 也是双射, 并且

$$(gf)^{-1} = f^{-1}h^{-1}. \tag{3}$$

证明 根据定理 2,f 的双射性导出了 f^{-1} 的存在性. 将条件 (1) 写成形式 $ff^{-1} = e_Y$, $f^{-1}f = e_X$, 它的对称性给出了等式 (2). 再根据定理 2, f^{-1} 也是双射. 其次, 由推论的条件和定理 2, 存在着映射

$$f^{-1}: Y \to X, \quad h^{-1}: Z \to Y$$

及其合成

$$f^{-1}h^{-1}: Z \to X.$$

由等式

$$(hf)(f^{-1}h^{-1}) = ((hf)f^{-1})h^{-1} = (h(ff^{-1}))h^{-1} = hh^{-1} = e_Z,$$

$$(f^{-1}h^{-1})(hf) = f^{-1}(h^{-1}(hf)) = f^{-1}((h^{-1}h)f) = f^{-1}f = e_X,$$

可以得到, $f^{-1}h^{-1}$ 是 fh 的逆映射. □

由法则 $\sigma(n) = n + 1$ 定义的映射 $\sigma: \mathbb{N} \to \mathbb{N}$ 是单射而不是满射, 因为第一个元素 1 不属于 $\mathrm{Im}\sigma$. 有趣的是对于有限集合, 类似情况不会出现.

定理 3 *如果 X 是有限集, 且变换 $f: X \to X$ 是单射, 则 f 是双射.*

证明 我们仅需指出 f 是满的, 即对任意元素 $x \in X$, 找到 x', 使得 $f(x') = x$. 令

$$f^k(x) = f(f \cdots (f(x)) \cdots) = f(f^{k-1}(x)), \quad k = 0, 1, 2, \cdots$$

由于 X 的有限性, 在这一序列中必有重复的元素. 设 $f^m(x) = f^n(x), m > n$. 若 $n > 0$, 由等式 $f(f^{m-1}(x)) = f(f^{n-1}(x))$ 和 f 的单射性, 得到 $f^{m-1}(x) = f^{n-1}(x)$.

重复地消去 f ，经过足够多次，我们得到等式

$$f^{m-n}(x) = f^0(x) = e(x) = x.$$

这时取 $x' = f^{m-n-1}(x)$ ，则 $f(x') = x$. □

易见，有限集合到自身的一个满变换也是双射.

下面对基数谈几句. 认为两个集合有相同的基数，当且仅当存在着双射 $f: X \to Y$, 与 $\mathbb{N}$(或 $\mathbb{Z}$) 基数相同的集合叫作 **可数集**.

习　题

1. 设 $\Omega = \{+, -, ++, +-, -+, --, +++, \cdots\}$ 是加号和减号的有限序列的集合，而 $f: \Omega \to \Omega$ 是一个变换，将元素 $\omega = \omega_1\omega_2\cdots\omega_n \in \Omega$ 对应到 $\omega' = \omega_1\dot{\omega}_1\omega_2\dot{\omega}_2\cdots\omega_n\dot{\omega}_n$ ，其中若 $\omega_k = +$ ，则 $\dot{\omega}_k = -$, 若 $\omega_k = -$, 则 $\dot{\omega}_k = +$. 证明在 $f(f\omega)$ 的长度 > 4 的任意区间内包含 $++$ 或 $--$.

2. 由法则 $n \to n^2$ 给出的映射 $f: \mathbb{N} \to \mathbb{N}$ 有右逆吗？给出 f 的两个左逆.

3. 设 $f: X \to Y$ 是一个映射，且 S,T 都是 X 的子集.
证明

$$f(S \cup T) = f(S) \cup f(T), \quad f(S \cap T) \subset f(S) \cap f(T).$$

试举一例，说明后一个式子中的包含关系一般来说不能换成相等关系.

4. 集合 S 的全体子集的集合记作

$$\mathcal{P}(S) = \{T | T \subset S\}.$$

例如若 $S = \{s_1, s_2, \cdots, s_n\}$ 是 n 个元素的有限集，则 $\mathcal{P}(S)$ 由空集 $\varnothing$,n 个单元集 $\{s_1\}, \{s_2\}, \cdots, \{s_n\}$, $n(n-2)/2$ 个二元集 $\{s_i, s_j\}$, $1 \leqslant i < j \leqslant n$, 等等，直到全集 $T = S$ 组成. 集合 $\mathcal{P}(S)$ 的基数是多少？

5. 设 $f: X \to Y$ 是一个映射，且设对某个元素 $a \in X$, $b = f(a)$. 原像

$$f^{-1}(b) = f^{-1}(f(a)) = \{x | f(x) = f(a)\}$$

叫作元素 $b \in \mathrm{Im} f$ 上的 **纤维**. 证明集合 X 是互不相交的纤维的并 (也就是说，给出了 X 的一个划分).

注意：符号 $f^{-1}(b)$ 不能联想到逆映射，后者可能并不存在.

6. 证明有限个可数集的笛卡儿积也是可数集.

7. 符号 $S \triangle T$ 表示两个集合 S 与 T 的 **对称差**:$S \triangle T = (S \backslash T) \cup (T \backslash S)$ (见图 6). 证明 $S \triangle T = (S \cup T) \backslash (S \cap T)$.

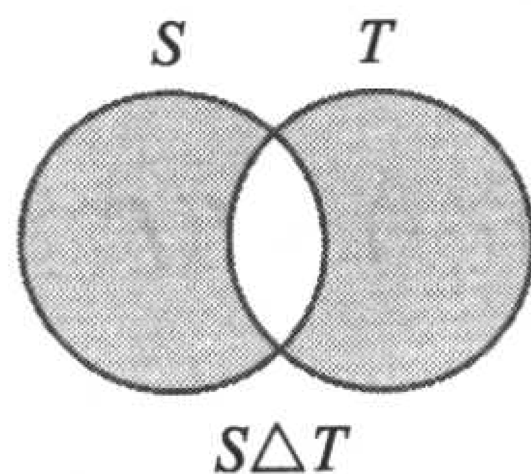


图 6

§6 等价关系. 商映射

在 §3 中引入的线性方程组的等价性，以及我们不自觉地在逻辑学，在日常生活等各个方面使用的各种形态的等价性使人们想到应该一般地定义这一概念.

1. 二元关系 设 X,Y 是任意两个集合，任意子集 $\omega\subset X\times Y$ 叫作 X 与 Y 之间的一个 **二元关系**.(若 $X=Y$，则简称为 X 上的一个二元关系.) 有序对 $(x,y)\in\omega$，用记号 $x\omega y$ 表示，并称 x 与 y 有关系 ω. 这种记法是方便的，例如实数集 $\mathbb{R}$ 中的顺序 $<$ 是 $\mathbb{R}$ 上的一个二元关系，由实平面 $\mathbb{R}^2$ 上位于直线 $x-y=0$ 上方的点组成 (见图 7); 用通常的不等式 $x<y$ 代替了繁琐的包含号 $(x,y)\in\omega$.

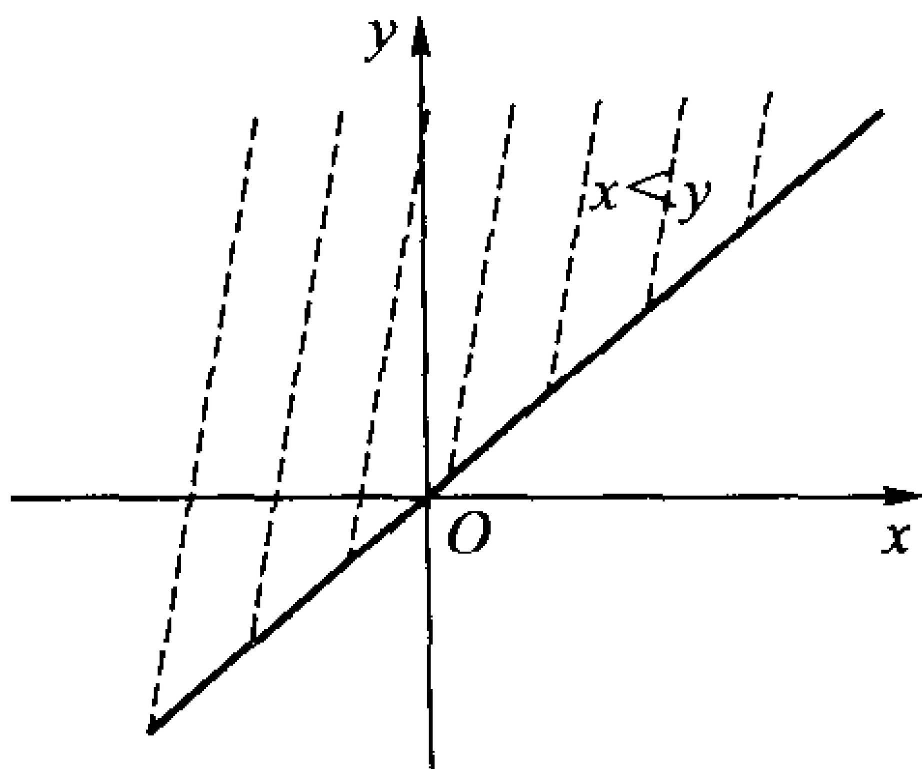


图 7

每一个函数 $f\colon X\to Y$ 都对应于它的图像，也就是子集

$$\Gamma(f)=\{(x,y)|x\in X,y=f(x)\}\subset X\times Y,$$

这是 X 与 Y 之间的一个二元关系. 研究函数 $\mathbb{R}\to\mathbb{R}$ 在 $\mathbb{R}^2$ 上的图像是数学分析的内容. 显然，并非每一个二元关系都可以作为某个映射 $X\to Y$ 的图像. 二元关系成为某个映射的图像的充要条件在于，任取 $x\in X$, 刚好有一个元素 y 使得 $x\omega y$. 事实上，给定 X,Y 和图像 $\Gamma(f)$, 可以重建映射 f.

2. 等价关系 集合 X 上的二元关系 $\sim$ 叫作 **等价关系**, 若任取 $x,x',x''\in X$，满足关系：

i) $x\sim x$(反身性);

ii) $x\sim x'\Rightarrow x'\sim x$ (对称性);

iii) $x\sim x',x'\sim x''\Rightarrow x\sim x''$ (传递性).

元素 $a,b\in X$ 不具有等价关系记作 $a\nsim b$.

与给定元素 x 等价的所有元素的子集

$$\bar{x}=\{x'\in X|x'\sim x\}\subset X$$

叫作包含 x 的 **等价类**. 由于 $x\sim x$ (见 (i)), 故确有 $x\in\bar{x}$. 任意元素 $x'\in\bar{x}$ 都叫作类 $\bar{x}$ 的 **代表元**.

下述论断成立.

命题　由关系 $\sim$确定的等价类的集合是集合 X 的一个划分，即 X 是这些子集的不交并 (记作 $\pi_\sim(X)$).

证明　事实上，$x \in \bar{x}$, 所以 $X = \cup_{x\in X}\bar{x}$. 现在如果 $\bar{x}' \cap \bar{x}'' \neq \varnothing$ 且 $x \in \bar{x}' \cap \bar{x}''$, 则 $x \sim x'$ 且 $x \sim x''$, 由传递性 (iii), 有 $x' \sim x''$, 以及 $\bar{x}' = \bar{x}''$, 这就意味着不同的等价类互不相交. □

设 $\Pi = \mathbb{R}^2$ 是带有直角坐标系的实平面.

将两点 $p,p' \in \Pi$ 属于同一条水平直线取作性质 $\sim$, 我们显然得到了一个等价关系，它的等价类是水平直线 (见图 8).

形如 $xy = \rho > 0$ 的双曲线 Γ_ρ 定义了区域 Π_+ 上的一个等价关系，其中 $\Pi_+ \subset \Pi$, 由点 $P(x,y)$, $x > 0, y > 0$ 组成 (见图 9). 这些几何例子直观地说明了下述逆命题成立.

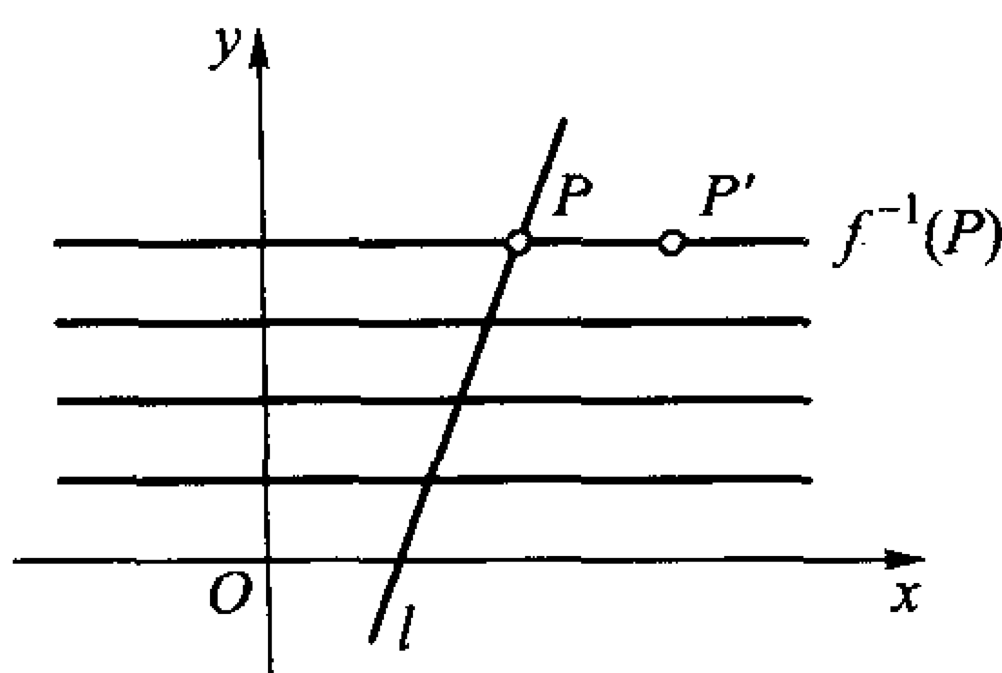


图 8

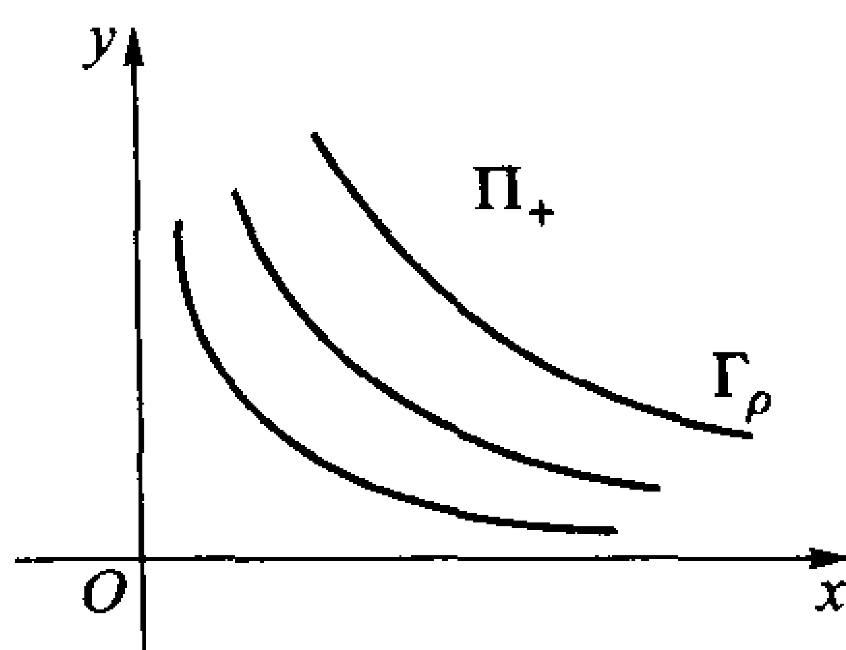


图 9

命题　如果 $\pi(X)$ 是将集合 X 分成不相交子集 C_x 的一个划分，则 C_x 是由某一等价关系 $\sim$ 确定的等价类.

证明　事实上，根据条件，每个元素 $x \in X$ 仅被包含在一个子集 C_a 中. 定义 $x \sim x'$ 当且仅当 x 与 x' 属于同一个子集 C_a . 显然，这个关系是反身，对称，且传递的，即 $\sim$ 是一个等价关系. 进一步根据定义，$x \in C_a \Rightarrow \bar{x} = C_a$. 所以 $\pi(X) = \pi_\sim(X)$. □

3. 商映射　由于上述给出的集合 X 的等价关系与划分之间的一一对应，对应于等价关系 $\sim$ 的划分通常记作 $X/\sim$, 并称之为 X 关于 $\sim$ 的商集 (或由关系 $\sim$ 确定的商集). 满射

$$p: x \mapsto p(x) = \bar{x} \tag{1}$$

叫作 X 到商集 $X/\sim$ 上的 **自然映射**(或 **典范投影**).

设 X, Y 是两个集合，且 $f: X \to Y$ 是一个映射. 二元关系 ω_f :

$$\forall X, x' \in X, \quad x\omega_f x' \Leftrightarrow f(x) = f(x')$$

显然是反身的 ($f(x) = f(x)$), 对称的 ($f(x') = f(x) \Rightarrow f(x) = f(x')$), 并且还是传递的 ($f(x) = f(x')$ 和 $f(x') = f(x'') \Rightarrow f(x) = f(x'')$). 这样 ω_f 是 X 上的一个等价关

系. 对应的等价类 $\bar{x}$ 就是在 §5 习题 5 意义下的纤维 (原像). 换言之

$$\bar{x}=\{x'|f(x')=f(x)\}.$$

映射 $f\colon X\to Y$ 诱导出一个映射 $\bar{f}\colon X/\omega_f\to Y$, 由法则

$$\bar{f}(\bar{x})=f(x),$$

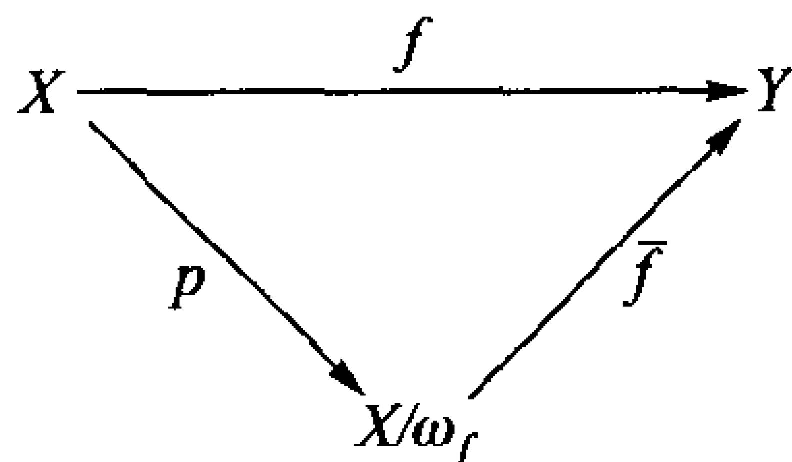
或

$$\bar{f}p(x)=f(x) \tag{2}$$

给出, 此处 p 是 (1) 式中给出的自然映射. 由于

$$\bar{x}=\bar{x}'\Leftrightarrow f(x)=f(x'),$$

所以给定 f, 关系式 (2) 不依赖于类 $\bar{x}$ 中代表元 x 的选取. 这时我们说 $\bar{f}$ 的定义是合理的(或良定义的). 交换图



直观地描述了一个分解式

$$f=\bar{f}\cdot p \tag{3}$$

映射 f 写成了一个满射 p 与一个单射 $\bar{f}$ 的乘积. $\bar{f}$ 的单性由下式给出

$$\bar{f}(\bar{x}_1)=\bar{f}(\bar{x}_2)\Leftrightarrow f(x_1)=f(x_2)\Leftrightarrow \bar{x}_1=\bar{x}_2.$$

显然 $\bar{f}$ 的满性等价于 f 的满性. 我们指出, 如果 $f'\colon X/\omega_f\to Y$ 是满足条件 (3) : $f'\cdot p=f$ 的另一个映射, 则由

$$f'(\bar{x})=f'(p(x))=(f'p)(x)=f(x)=\bar{f}(\bar{x})$$

(见公式 (2)) 得到等式 $f'=\bar{f}$. 因而上述三角交换图中给出的映射 $\bar{f}$ 是唯一确定的.

4. 序集 一个**有序集**X(或集合 X 上的一个序) 指 X 上的一个二元关系 $\leqslant$, 满足反身性 ($x\leqslant x$), 反对称性 (若 $x\leqslant y$ 且 $y\leqslant x$, 则 $x=y$) 和传递性 (若 $x\leqslant y, y\leqslant z$, 则 $x\leqslant z$). 当 $x\leqslant y$ 且 $x\neq y$ 时, 记作 $x<y$. $x\leqslant y$ 也可以用记号 $y\geqslant x$ 表示. 一对元素 $x,x'\in X$ 可能没有 $\leqslant$ 关系. 但是如果对于 X 的每一对元素都有 $x\leqslant x'$ 或 $x'\leqslant x$, 则称 X 为**线性序集**或**全序集**. 在一般情况下, 称 X 上有一个**偏序**.

给出偏序集的两个例子. 集合 S 的子集的集合 $\mathcal{P}(S)$ (见 §5 习题 4) 连同通常的子集之间的包含关系 $R \subset T$ 是一个偏序集. 而自然数集 $\mathbb{N}$ 连同关系 $d|n$(n 被 d 整除) 也是一个 偏序集.

设 X 是一个偏序集, x 和 y 是 X 的元素. 称 y **紧跟**(或 **覆盖**)x, 如果 $x < y$, 且不存在元素 z, 使得 $x < z < y$. 在 $\text{Card}X < \infty$ 的情况下, $x < y$(即 x 与 y 是可比的) 当且仅当可以找到一个元素列 $x = x_1, x_2, \cdots, x_{n-1}, x_n = y$, 其中 x_{i+1} 紧跟 x_i. 紧跟的概念可以用于绘制有限偏序集的平面图. 用点表示集合 X 的元素. 若 y 紧跟 x, 则把 y 放在高于 x 的位置上, 并将 x 与 y 用直线段连接起来. y 与 x 的可比性表现为连接 y 和 x 的一条下降的折线, 这样的折线可能同时有几条, x 与 y 是不可比的则没有折线连接.

在图 10 的前两个图中描述了自然序数的 "线段" 以及集合 $\mathcal{P}(\{a,b,c\})$($\mathbb{N}$ 是自然的线性序集, 而 $\mathcal{P}(S)$ 的序已在上面给出).

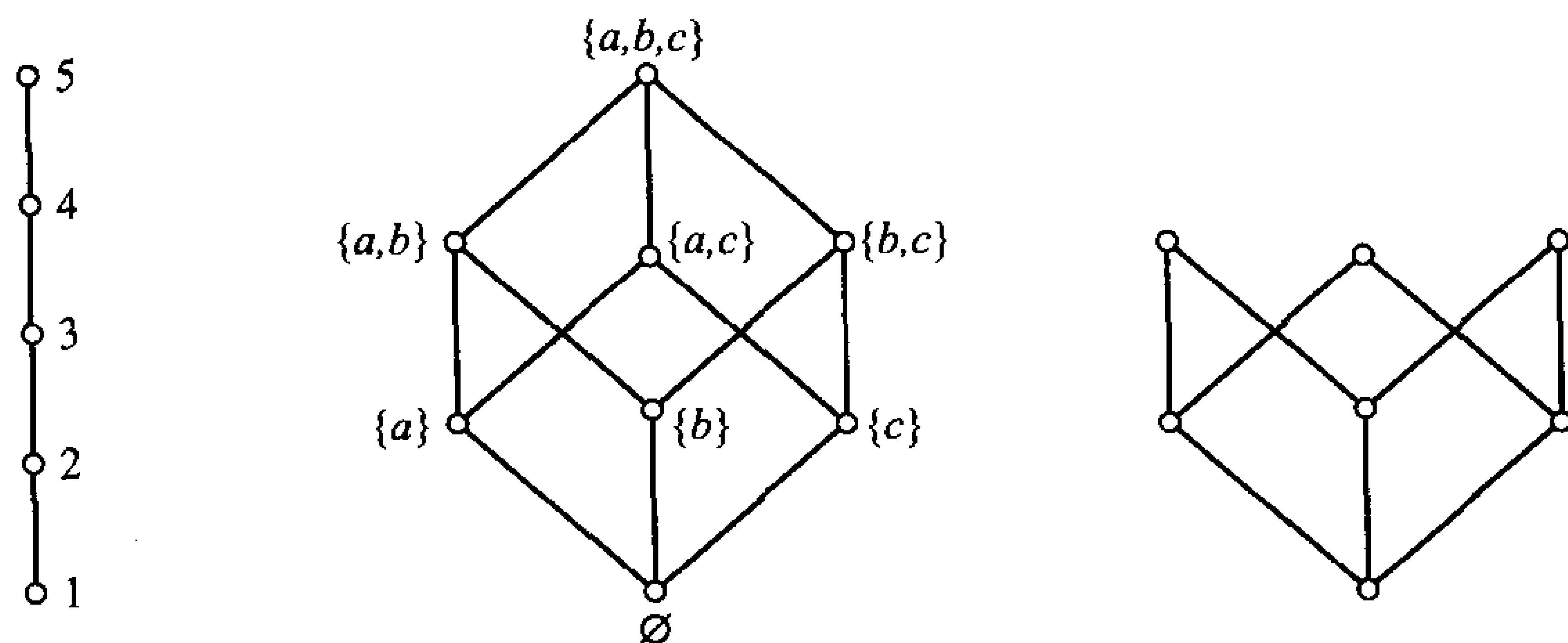


图 10

一个偏序集 X 的 **最大元** 指元素 $n \in X$, 使得任取 $x \in X$, 都有 $x \leqslant n$, 而 **极大元** 指元素 $m \in X$, 使得从 $m \leqslant x \in X$ 可得 $x = m$. 最大元永远是极大的, 但反之不真. 极大元可以有很多个, 但最大元如果存在的话, 必定是唯一确定的. 相应地可以定义 **最小元** 和 **极小元**. 在图 10 中, 左边的两个图有最大元和最小元, 右边的图有三个极大元 (一个最小元), 但没有最大元.

偏序代数系统的理论 (布尔代数, 格论) 充满了丰富的结果并在代数学中占有重要地位, 但我们不可能去涉及它. 本段的目的仅在于使读者认识自然的二元关系并提供图解, 它将有助于理解在群当中子群或者域当中子域的相互位置.

习　题

1. 设 $\mathbb{R}^2/\sim$ 是图 8 中给出的商集, l 是与 OX 轴相交的任意直线, 试给出 $\mathbb{R}^2/_\sim$ 的元素与 l 的点之间的一一对应.

2. 令实坐标平面 $\mathbb{R}^2$ 上的两点 $P(x,y) \sim P(x',y')$, 当且仅当 $x'-x \in \mathbb{Z}$ 且 $y-y' \in \mathbb{Z}$. 证明 $\sim$ 是等价关系, 且商集可以几何地表示为环面 (例如小面包圈的表面, 见图 11) 上的点集.

3. 证明 2 元、3 元和 4 元集分别有 2,5 和 15 个不同的商集.

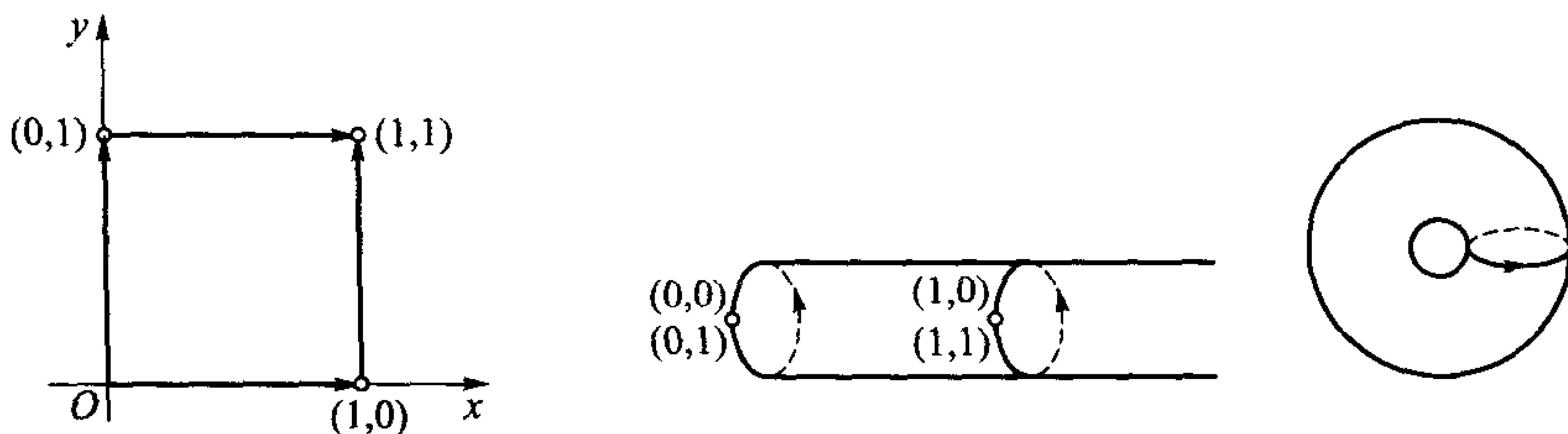


图 11

4. 设 $\sim$ 是集合 X 上的一个等价关系，且 $f: X \to Y$ 是一个映射，使得

$$x \sim x' \Rightarrow f(x) = f(x')$$

证明 f 与 $\sim$ 的这一相容性条件 (比第 2 段讨论的条件要弱) 允许我们定义一个从 $X/\sim$ 到 Y 的诱导映射 $\bar{f}: \bar{x} \mapsto f(x)$，它给出了分解式 $f = \bar{f} \cdot p$, 但 $\bar{f}$ 不一定是单射. $\bar{f}$ 成为单射的条件是什么？

5. 画出下述偏序集的图解：

1) $\mathcal{P}(\{a,b,c,d\})$;

2) 整数 24 的全体因子的集合 (偏序关系由整除给出).

§7 数学归纳法原理

假设读者对全体 *自然数*(或 *正整数*) 的集合 $\mathbb{N} = \{1,2,3,\cdots\}$ 了解得很清楚. 事实上，研究集合 $\mathbb{N}$ 的出发点是皮亚诺公理 (皮亚诺，1858—1932). 从皮亚诺公理可以推导出自然数集，更精确地，非负整数集中加法和乘法的性质以及线性序 (见 §6 第 4 段). 特别是证明了一个直观而清晰的论断： *每一个非空集合 $S \subset \mathbb{N}$ 都有最小元*，即存在一个自然数 $s \in S$, 它小于 S 中的所有的数. 根据皮亚诺公理得到的这一论断推导出下述

归纳法原理 *假设对每一个 $n \in \mathbb{N}$，我们有某一命题 $M(n)$. 又假设我们有一个法则，对于任意给定的 l，只要 $M(k)$ 对所有的 $k < l$ 真就可以证明 $M(l)$ 真，特别指出，我们能够验证 $M(l)$ 真.*

则对任意的 $n \in \mathbb{N}, M(n)$ 真.

事实上，设子集

$$S = \{s | s \in \mathbb{N}, M(s) \text{ 不真}\} \subset \mathbb{N}$$

不是一个空集. 按照上述讨论，S 包含有一个最小元 s_0. 这时论断 $M(s_0)$ 不真，而对任意的 $s < s_0, M(s)$ 真. 这就和我们在假设条件下能够证明 $M(s_0)$ 真矛盾.

此处我们不能对数学归纳法原理进行全面的讨论. 而仅局限于指出它反映了自然数列的本质，对自然数列的认识不能再归结到本质上更简单的事实了. 再次将注意力转到归纳法. "完全归纳法证明" 必不可少的一步是 *归纳的基础*, 即性质或命题

对某些不太大的 n 成立. 缺少这一验证, 就可能推出类似于 "所有的学生都一样高" 的随意性命题. 论证如下. 空集和一个学生的集合具有这一性质. 给出归纳假设, 即任意学生数 $\leqslant n$ 的集合具有这一性质. 则在 $(n+1)$ 个学生的集合中, 根据归纳假设, 前 n 个学生和后 n 个学生的身高相同. 这两个集合有一个有 $n-1$ 个身高相同的学生的子集. 因此所有的 $n+1$ 个学生身高相同. 事实上, 第一步有意义的论断应当对任意两个学生的集合给出, 而它恰好是不对的. 归纳的基础取多长才够呢? 一般来说, 这件事从证明中就可以清楚地看出来. 在我们这个初等例子中, 重要的条件是两个集合的交不空, 即不等式 $n-1\geqslant 1$ 成立, 从而 $n\geqslant 2$.

在更复杂的情况下, 特别是当我们借助递推关系用归纳法定义或构造一个对象时, 必须对归纳基础格外关心. 例如脚标可以被 5 整除的斐波那契数 f_{5m}(见 §3, 例 2, 此处 $m\geqslant 1$) 可以由等式 $f_5=5$ 及其递推关系 $f_{5(m+1)}=5f_{5m+1}+3f_{5m}$ 导出, 首先得到的是归纳基础. 另一方面, 也不能陷入另一个极端: 对充分长的自然数列 $1\leqslant k\leqslant l$ 中的一切 k 验证 $M(k)$ 的正确性, 然后作出没有根据的结论, 对一切 $n\in\mathbb{N}$,$M(n)$ 真 (称这一作法为 *不完全归纳法*).

在这里给出两个令人不愉快的例子.

例 1 费马猜想, 所有形如 $F_n=2^{2^n}+1$ 的 **费马数** 都是素数, 此处 $n=0,1,2,\cdots$. 前 5 个费马数是素数. 但欧拉找到了 F_5 的一个分解式: $F_5=4\,294\,967\,297=641\cdot 6700417$. 人们执拗地企图在最新式计算机的帮助下找到哪怕一个新的费马素数, 但直到现在也没有成功. 这一方向的最新 "成果" 是验证了 F_{1945} 可以被 $5\cdot 2^{1947}+1$ 整除.

例 2 观察当 $n=1,2,\cdots,40$ 时, 形如 n^2-n+41 的数 (这是欧拉研究的一个多项式), 人们可能会猜想这个多项式对任意 n 都得到素数 (关于素数见 §9). 但是 $41^2-41+41=41^2$.

这种类型的例子要多少有多少.

在用归纳法研究问题时, 有时最重要的事情是, 使所证的论断具有恰当的形式. 假设要求和式

$$\mathbf{p}_k(n)=1^k+2^k+3^k+\cdots+(n-1)^k+n^k,\quad k=1,2,3.$$

如果告诉我们, 答案包含在下述表达式中, 问题就大大简化了

$$\mathbf{p}_1(n)=\frac{n(n+1)}{2},\quad \mathbf{p}_2(n)=\frac{n(n+1)(2n+1)}{2},\quad \mathbf{p}_3(n)=\left[\frac{n(n+1)}{2}\right]^2.$$

幂和 $\mathbf{p}_k(n)$ 的一般形式将联系到多项式的根再一次进行讨论 (见第 6 章), 此刻我们指出, 在 §3 第 5 段中遇到的公式 $\Gamma(n)$ 有下述形式

$$\begin{aligned}\Gamma(n)&=n(n-1)+\cdots+k(k-1)+\cdots+1(1-1)\\&=\sum_{k=1}^{n}k^2-\sum_{k=1}^{n}k=\mathbf{p}_2(n)-\mathbf{p}_1(n)\end{aligned}$$

(今后将会经常用到求和号 $\sum$). 基于上述 $\mathbf{p}_2(n)$ 和 $\mathbf{p}_1(n)$ 的表达式, 我们得到 $\Gamma(n) = (n^3 - n)/3$. 显然这一结果可以直接对 $\Gamma(n)$ 作归纳论证得到.

如果说想出 $\mathbf{p}_1(n)$ 的形式不太困难, 那么想出 $\mathbf{p}_2(n)$, $\mathbf{p}_3(n)$ 的形式就没那么平凡了, 而关系式

$$\mathbf{p}_5 + \mathbf{p}_7 = 2\left(\frac{n(n+1)}{2}\right)^2$$

一般需要按照某种确定的步骤寻找. 目前这样的步骤是能够给出的, 但我们在这里不考虑它. 而证明上述已经给出的对应关系, 只需要直接计算从 n 到 $n+1$ 的一步归纳. 我们把它留给读者作为有益的练习.

恰好在这一练习中用到下述 **二项式公式**

$$(a+b)^n = a^n + \begin{pmatrix} n \\ 1 \end{pmatrix} a^{n-1}b + \cdots + \begin{pmatrix} n \\ k \end{pmatrix} a^{n-k}b^k + \cdots + b^n \tag{1}$$

此处 a 和 b 是任意数, 而单项式 $a^{n-k}b^k$ 的 **二项式系数** $\begin{pmatrix} n \\ k \end{pmatrix}$ 形如

$$\begin{pmatrix} n \\ k \end{pmatrix} = \frac{n!}{k!(n-k)!} = \frac{n(n-1)\cdots(n-k+1)}{k(k-1)\cdots 2,1}, \tag{2}$$

这里 $n! = n(n-1)\cdots 2.1$(n 的阶乘). 其值快速增长, 例如 $6! = 720, 10! = 3628800$, 而 $100! > 10^{150}$. 对公式 (2) 进行补充, 允许 $0! = 1$ 以及当 $k < 0$ 时 $\begin{pmatrix} n \\ k \end{pmatrix} = 0$ 是有益处的. 我们还要指出,

$$\begin{pmatrix} n \\ n-k \end{pmatrix} = \begin{pmatrix} n \\ k \end{pmatrix}$$

(二项式系数的对称性).

当 $n = 1, 2$ 时, 公式 (1) 显然成立, 我们对 n 作归纳. 假设公式对所有 $\leqslant n$ 的数成立, 用 $a+b$ 去乘 (1) 式的两端, 我们有

$$\begin{aligned}
&(a+b)^{n+1} = (a+b)^n(a+b) \\
&= a^n(a+b) + \cdots + \begin{pmatrix} n \\ k \end{pmatrix} a^{n-k}b^k(a+b) + \cdots + b^n(a+b) \\
&= a^{n+1} + a^n b + \cdots + \begin{pmatrix} n \\ k-1 \end{pmatrix} a^{n+2-k}b^{k-1} + \begin{pmatrix} n \\ k-1 \end{pmatrix} a^{n+1-k}b^k \\
&\quad + \begin{pmatrix} n \\ k \end{pmatrix} a^{n+1-k}b^k + \begin{pmatrix} n \\ k \end{pmatrix} a^{n-k}b^{k+1} + \cdots + ab^n + b^{n+1}.
\end{aligned}$$

合并同类项，单项式 $a^{n+1-k}b^k$ 的系数为

$$\begin{aligned}&\binom{n}{k-1}+\binom{n}{k}\\&=\frac{n!}{(k-1)!(n-k+1)!}+\frac{n!}{k!(n-k)!}\\&=\frac{n!}{(k-1)!(n-k)!}\left[\frac{1}{n-k+1}+\frac{1}{k}\right]\\&=\frac{n!}{(k-1)!(n-k)!}\cdot\frac{n+1}{k(n-k+1)}\\&=\frac{(n+1)!}{k!(n+1-k)!}=\binom{n+1}{k},\end{aligned}$$

即恰好对形如 (2) 的二项式系数的上指标增加 1. 这就证明了公式对一切 $n\in\mathbb{N}$ 成立.

如果写成

$$(a+b)^n=(a+b)(a+b)\cdots(a+b),$$

给右边的因子从 1 到 n 编号，并考察所有的编号为

$$1\leqslant i_1<i_2<\cdots<i_k\leqslant n$$

的子集，它们与乘积中的单项式 $a^{n-k}b^k$ 相符，所以我们断言，$\binom{n}{k}$ 恰为 n 元集中所有 k 元子集的个数. 比较老式的术语是从 n 个元素中每次取 k 个元素的组合数

$$\mathrm{C}_n^k=\binom{n}{k},$$

这是一种本质上的表述.

特别地，集合 $\mathcal{P}(\{s_1,\cdots,s_n\})$ (见 §5 习题 4) 的基数等于

$$\binom{n}{0}+\binom{n}{1}+\cdots+\binom{n}{n-1}+\binom{n}{n}.$$

在公式 (1) 中令 $a=b=1$, 我们得到

$$2^n=\binom{n}{0}+\binom{n}{1}+\binom{n}{2}+\cdots+\binom{n}{n-1}+\binom{n}{n}.$$

于是，

$$\operatorname{Card}\mathcal{P}(\{s_1,s_2,\cdots,s_n\})=2^n.$$

二项式系数在初等组合论中几乎是必不可少的. 下面是一个直观的几何例子.

例 (美国数学月刊, 1977,V.84,No.6) 给定圆周上任意 n 个点, 确定由 $\binom{n}{2}$ 条弦划分的圆内的区域数 R_n. 此处假设任意三条弦在圆内不相交 (见图 12). 这是一个著名的问题.

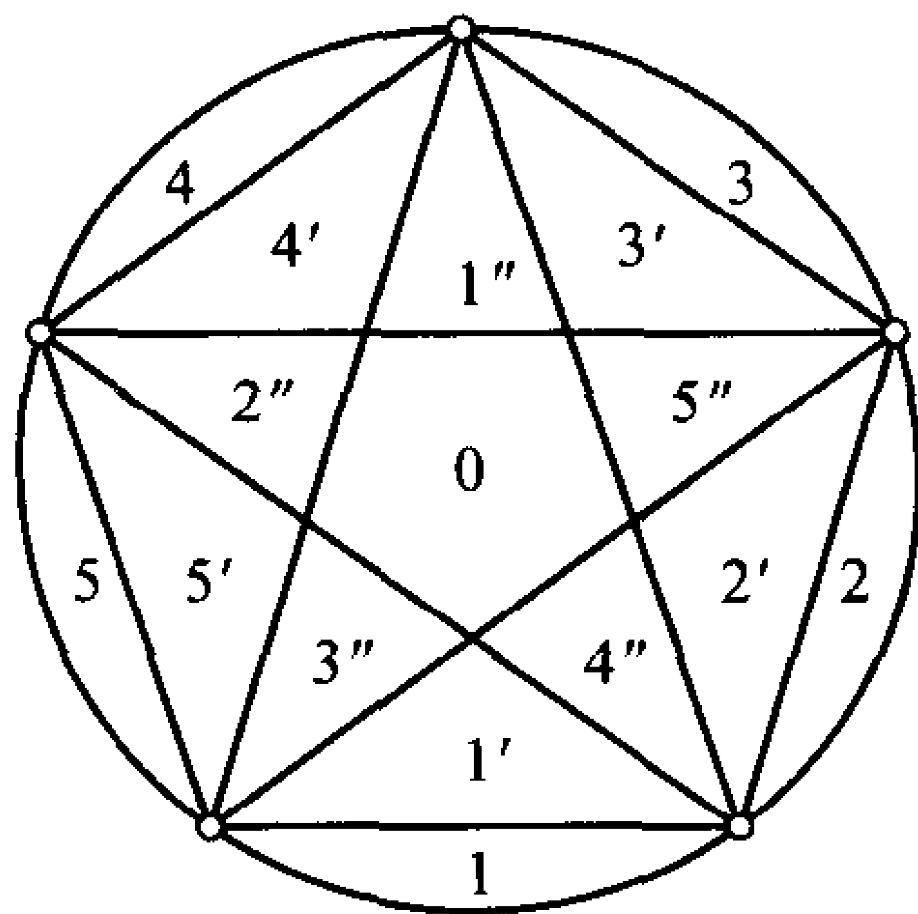


图 12

当 $n = 1,2,3,4,5$ 时的结果使人们想到 $R_n = 2^{n-1}$, 但事实上, 正确的公式为 $R_n = 1 + \binom{n}{2} + \binom{n}{4}$. 试证明之.

证明定理或构造数学对象时, 有时需要借助更复杂的归纳形式. 例如下面的二重归纳原理. 设任取自然数 m 和 n, 有某一命题 $Y(m,n)$, 并且:

i) $Y(m,1)$ 和 $Y(1,n)$ 对所有的 m,n 真;

ii) 如果 $Y(k-1,l)$ 和 $Y(k,l-1)$ 真, 则 $Y(k,l)$ 亦真.

(这就等价于说:

ii′) 如果对一切满足 $k' \leqslant k,\ l' \leqslant l, k'+l' < k+l$ 的数对 $(k',l'),Y(k',l')$ 真, 则 $Y(k,l)$ 亦真.)

那么命题 $Y(m,n)$ 对所有的自然数 m 和 n 都真.

习　　题

1. 令

$$s(n) = \sin\varphi + \sin 2\varphi + \cdots + \sin n\varphi,$$
$$c(n) = \cos\varphi + \cos 2\varphi + \cdots + \cos n\varphi.$$

对 n 作归纳证明公式

$$s(n) = \frac{\sin(n\varphi/2)\sin((n+1)\varphi/2)}{\sin(\varphi/2)}, c(n) = \frac{\sin(n\varphi/2)\cos((n+1)\varphi/2)}{\sin(\varphi/2)}.$$

2. 下述公式成立:

a) $\displaystyle\sum_{k=1}^{n} \cot^2\left(\frac{k\pi}{2n+1}\right) = \frac{n(2n-1)}{3}$;

b) $\displaystyle\sum_{k=0}^{n} \binom{2k}{n}\binom{2n-2k}{n-k} = 4^n$.

至少在 $n \leqslant 5$ 时，验证它们的正确性.

§8 置换

1. 置换的标准记法 我们来进一步讨论 §5 提出的关于有限集一一变换的几个问题. 一些重要的代数概念就是在这一基础上自然产生的.

令 Ω 是 n 元有限集. 由于元素的性质对于我们来说是非本质的，为方便起见，不妨设 $\Omega=\{1,2,\cdots n\}$. 由 $\Omega\to\Omega$ 的全体一一变换组成的集合记作 S_n=$S(\Omega)$，其元素通常用小写希腊字母表示，称为 **置换**. 仅对恒等映射 $e=e_\Omega$ 保留用拉丁字母.

用展开和直观的方式将任意置换 π: $i\mapsto\pi(i), i=1,2,\cdots,n$，表示成下述形式:

$$\pi=\begin{pmatrix}1 & 2 & \cdots & n\\ i_1 & i_2 & \cdots & i_n\end{pmatrix},$$

它完全指明了所有的像:

$$\begin{array}{cccccc} & 1 & 2 & \cdots & n & \\ \pi & \downarrow & \downarrow & & \downarrow & , \\ & i_1 & i_2 & \cdots & i_n, & \end{array}$$

其中 $i_k=\pi(k), k=1,2,\cdots,n$, 是符号 $1,2,\cdots,n$ 的一个排列.

设置换 $\sigma,\tau\in S_n$, 它们的乘法对应于映射合成的一般法则: $(\sigma\tau)(i)=\sigma(\tau(i))$. 例如对于置换

$$\sigma=\begin{pmatrix}1&2&3&4\\2&3&4&1\end{pmatrix},\quad \tau=\begin{pmatrix}1&2&3&4\\4&3&2&1\end{pmatrix}$$

我们有

$$\sigma\tau=\begin{pmatrix}1&2&3&4\\2&3&4&1\end{pmatrix}\begin{pmatrix}1&2&3&4\\4&3&2&1\end{pmatrix}=\begin{array}{cccc}1&2&3&4\\ \downarrow&\downarrow&\downarrow&\downarrow\\ 4&3&2&1\\ \downarrow&\downarrow&\downarrow&\downarrow\\ 1&4&3&2\end{array}=\begin{pmatrix}1&2&3&4\\1&4&3&2\end{pmatrix}.$$

同时

$$\tau\sigma=\begin{pmatrix}1&2&3&4\\4&3&2&1\end{pmatrix}\begin{pmatrix}1&2&3&4\\2&3&4&1\end{pmatrix}=\begin{pmatrix}1&2&3&4\\3&2&1&4\end{pmatrix},$$

所以 $\sigma\tau\neq\tau\sigma$.

按照 §5 的结果，置换的乘法满足下述规律.

i) 乘法是结合的: 对任意 $\alpha,\beta,\gamma\in S_n,(\alpha\beta)\gamma=\alpha(\beta\gamma)$.

ii) S_n 有单位元 e: 对任意 $\pi \in S_n, \pi e = \pi = e\pi$.

iii) 每一个元素 $\pi \in S_n$ 都有逆元 $\pi^{-1} : \pi\pi^{-1} = e = \pi^{-1}\pi$.

这三条性质，补上我们暂且不谈的一般法则 (见第 4 章), 给出了称 S_n 为群的根据. 准确地说，集合 S_n 连同其元素的自然乘法运算 (置换的合成), 叫作 **n 元对称群**(或 n 个符号的对称群, 或 n 个点的对称群). 对于我们来说，眼下不过是术语上的约定，它将重点从集合 S_n 转向了同样重要的置换的乘法性质，即转向 S_n 中元素的合成可能表现出来的性质. 对称群 S_n 是群的一般理论和 170 多年前伽罗瓦理论的源头，而且大量的数学思想正是与它相联系才得以产生.

注记 如果将术语置换当作数字 $1, 2, \cdots, n$ 按照某种顺序摆放的代名词，S_n 的元素有时也称为 **排列**(подстановка). 因为 n 元有序数列与 S_n 的元素之间存在着一一对应，而 “置换” 一词比固定的序列使人更快地联想到运算，所以排列一词就不再使用了，我们后面还会谈到，例如将数代入 [①] 多项式，但是它仅作为所指含义的另外规定.

如果还需要更多的出处，至少可以在 a) 科学文献； b) П. С. 亚历山大罗夫的教科书《解析几何讲义》 (Наука (科学出版社),1968,c 767) 中找到.

我们来计算群 S_n 的阶 $|S_n|$. 符号 1 在置换 σ 的作用下变成了符号 $\sigma(1), \sigma(1)$ 有 n 种不同的取法，确定了 $\sigma(1), \sigma(2)$ 只能从剩下的 $n-1$ 个符号中去取 (所以不同的对 $(\sigma(1), \sigma(2)$) 共计有 $(n-1)+(n-1)+\cdots+(n-1)=n(n-1)$ 个), 而 $\sigma(3)$ 只能从 $n-2$ 个符号中取等等. $\sigma(1), \sigma(2), \cdots, \sigma(n)$ 的所有可能的选择，也就是所有不同的置换共计 $n(n-1)\cdots 2, 1 = n!$ 个. 所以

$$\text{Card } S_n = |S_n| = n!$$

2. 置换的循环结构 我们现在将 S_n 中的置换分解为更简单的置换的乘积. 先用上例中的置换 $\sigma, \tau \in S_4$, 能过图表 (图 13) 说明分解的思路.

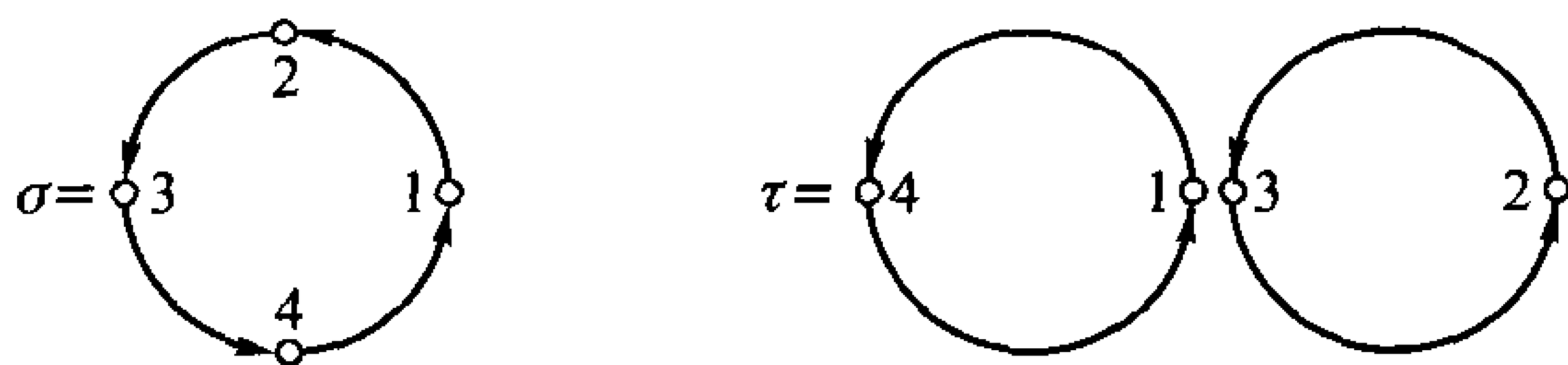


图 13

置换 σ 叫作一个 长为 4 的循环, 简单地写成 $\sigma = (1 \quad 2 \quad 3 \quad 4)$, 或

$$\sigma = (2 \quad 3 \quad 4 \quad 1) = (3 \quad 4 \quad 1 \quad 2) = (4 \quad 1 \quad 2 \quad 3),$$

而置换

$$\tau = (1\,4)\,(2\,3)$$

① 作者这样说是因为在俄文中代入与排列是同一个词. —— 译者注.

是两个*无关的*(*不相交的*) 长为 2 的循环 (1 4) 和 (2 3) 的乘积. 我们指出

$$\sigma^2 = (1\ 3)\ (2\ 4), \sigma^4 = (\sigma^2)^2 = e, \tau^2 = e.$$

现在设 π 是 S_n 中的任意置换. 其方幂 π^s 归纳地定义如下 (见 §5 定理 3 的证明)：

$$\pi^s = \begin{cases} \pi(\pi^{s-1}), & 若\ s > 0, \\ e, & 若\ s = 0, \\ \pi^{-1}((\pi^{-1})^{(-s-1)}), & 若\ s < 0. \end{cases}$$

这时显然有

$$\pi^s\pi^t = \pi^{s+t} = \pi^t\pi^s, s, t \in \mathbb{Z}$$

(当 s 与 t 同号时，顺序添上 π 或 π^{-1}，当 s 与 t 异号时，用 e 代替 $\pi\pi^{-1}, \pi^{-1}\pi$). 因为 $|\Omega| < \infty$，所以对于每一个置换 $\pi \in S_n$，可以找到唯一确定的自然数 $q = q(\pi)$，使得全部不同的方幂包含在集合 $\langle\pi\rangle = \{e, \pi, \cdots, \pi^{q-1}\}$ 中，且 $\pi^q = e$. 该数 q 叫作置换 π 的 **阶**. 这样，上述置换 σ 和 τ 分别有阶 4 和 2.

称两个点 $i, j \in \Omega$ 为*π等价的*, 若存在某个 $s \in \mathbb{Z}$，使得 $j = \pi^s(i)$. 因为

$$i = \pi^0(i), j = \pi^s(i) \Rightarrow i = \pi^{-s}(j), j = \pi^s(i), k = \pi^t(j) \Rightarrow k = \pi^{s+t}(i),$$

我们显然得到了 Ω 上的一个关系，它具有反身、对称、传递性 (见 §6 第 2 段). 基于等价关系的一般性质，我们有

$$\Omega = \Omega_1 \cup \cdots \cup \Omega_p. \tag{1}$$

集合 Ω 划分成了两两不相交的类 $\Omega_1, \cdots, \Omega_p$，这些类被直观地称为 π **轨道**. 这一名称是完全有根据的：因为每一个点 $i \in \Omega$ 恰属于一个轨道，并且如果 $i \in \Omega_k$, 则 Ω_k 由元素 π 的方幂作用在点 i 上的像组成： $i, \pi(i), \pi^2(i), \cdots, \pi^{l_k-1}(i)$，此处 $l_k = |\Omega_k|$ 是*π轨道 Ω_k 的长度*. 显然

$$l_k \leqslant q = \mathrm{Card}\langle\pi\rangle, \quad \pi^{l_k}(i) = i,$$

并且 l_k 是具有这些性质的最小数. 令

$$\pi_k = (i, \pi(i), \cdots, \pi^{l_k-1}(i)) = \begin{pmatrix} i & \pi(i) & \cdots & \pi^{l_k-2}(i) \\ \pi(i) & \pi^2(i) & \cdots & \pi^{l_k-1}(i) \end{pmatrix},$$

我们得到了一个置换，叫作*长为 l_k 的循环*.

将循环写成 $(1\ 2\ 3 \cdots l\ )$ 或 $(1, 2, 3, \cdots, l)$ 是有趣和方便的.

循环 π_k 使集合 $\Omega \backslash \Omega_k$ 中所有的点保持不变，而任取点 $j \in \Omega_k$, $\pi(j) = \pi_k(j)$ 这一性质给我们提供了称两个循环 $\pi_s, \pi_t, s \neq t$，是*无关的*或*不相交的*这一说法的依据. 因为任取 $i \in \Omega_k$, $\pi_k^{l_k}(i) = i$，所以 $\pi_k^{l_k} = e$.

这样，公式 (1) 的划分对应于置换 π 到乘积的分解

$$\pi = \pi_1\pi_2\cdots\pi_p, \tag{2}$$

其中任意两个循环都是可换序的： $\pi = \pi_1\pi_2\cdots\pi_p = \pi_{l_1}\pi_{l_2}\cdots\pi_{l_p}$. 可以假定 $l_1 \geqslant l_2 \geqslant \cdots \geqslant l_m > l_{m+1} = \cdots = l_p = 1$.

如果循环 $\pi_k = (i)$ 的长度是 1, 那么它事实上是恒等置换. 这样的循环自然可在乘积 (2) 中省略：

$$\pi = \pi_1\pi_2\cdots\pi_m, \quad l_k > 1, \quad 1 \leqslant k \leqslant m. \tag{3}$$

例如我们可以将置换

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 4 & 5 & 1 & 7 & 6 & 8 \end{pmatrix} \in S_8$$

写成

$$\pi = (1\ 2\ 3\ 4\ 5)(6\ 7)(8) = (1\ 2\ 3\ 4\ 5)(6\ 7). \tag{4}$$

对任意 $n \geqslant 7$,(1 2 3 4 5)(6 7) 可以看成 S_n 的置换，这是上述记号的不便之处，可是一旦 n 确定下来，这种不确定性就不存在了.

更精确地，假设我们还有形如 (3) 式的另一种分解 $\pi = \alpha_1\alpha_2\cdots\alpha_r$, 它也是不相交循环的乘积，并设符号 i 在 π 的作用下改变. 这时存在 $\pi_1, \cdots, \pi_m$ 中的一个 (且仅有一个) 循环 π_s , 使得 $\pi_s(i) \neq i$, 同时，存在 $\alpha_1, \cdots, \alpha_r$ 中的一个循环 α_t , 使得 $\alpha_t(i) \neq i$. 我们有 $\pi_s(i) = \pi(i) = \alpha_t(i)$. 如果我们已经知道

$$\pi_s^k(i) = \pi^k(i) = \alpha_t^k(i), \tag{5}$$

那么将置换 π 作用于这一等式，并运用 π 与 π_s^k 和 α_t^k 的交换性，我们得到

$$\pi\pi_s^k(i) = \pi^{k+1}(i) = \pi\alpha_t^k(i),$$

因而 $\pi_s^k\pi(i) = \pi^{k+1}(i) = \alpha_t^k\pi(i)$, 最后,

$$\pi_s^{k+1}(i) = \pi^{k+1}(i) = \alpha_t^{k+1}(i).$$

这就是说，等式 (5) 对任意 $k = 0, 1, 2, \cdots$ 成立. 但循环是被它的方幂在任意一个发生改变的符号上的作用唯一确定的. 因而 $\pi_s = \alpha_t$. 然后再对 m 或 r 用归纳法.

于是我们证明了

定理 1 S_n 中的每一个置换 $\pi \neq e$ 都是长度 $\geqslant 2$ 、不相交的循环的乘积. 这一分解式精确到循环的顺序是唯一确定的.

将注意力转到长为 2 的循环.

定义 长为 2 的循环叫作 **对换**.

任意对换的形状为 $\pi = (i\ j)$, 它不改变所有异于 i, j 的符号. 从定理 1 得到

推论 每一个置换 $\pi \in S_n$ 都是对换的乘积.

证明 事实上, 循环可以写成对换的乘积, 例如

$$(1\quad 2\quad \cdots\quad l-1\quad l) = (1\quad l)(1\quad l-1)\cdots(13)(12).$$

而定理 1 保证了任意置换可写成对换的乘积. □

对定理 1 及其推论中的公式说明如下. 从循环 $\sigma = (i_1\, i_2\, i_3 \cdots i_{l-1}\, i_l)$ 的定义得出

$$i_1 \mapsto i_2,\ i_2 \mapsto i_3,\ \cdots,\ i_{l-1} \mapsto i_l,\ i_l \mapsto i_1$$

和

$$j \mapsto j, j \in \Omega \backslash \{i_1, i_2, \cdots, i_{l-1}, i_l\},$$

如果我们将 σ 写成 $\sigma = (i_2\ \ i_3 \cdots i_l\ \ i_1)$, 即对包含在 σ 中的号码循环移位, 则任何事情都没有改变. 这样, 定理 1 的唯一性是一个本质的特性. 另一方面, 在推论中将置换写成对换的乘积是没有这种唯一性的. 令

$$\sigma = (i_1\ \ i_2\ \ i_3 \cdots i_{l-1}\ \ i_l) = (i_1\, i_l)(i_1\, i_{l-1}) \cdots (i_1\, i_3)(i_1\, i_2),$$
$$\sigma = (i_2\ \ i_3 \cdots i_{l-1}\ \ i_l\ \ i_1) = (i_2\, i_1)(i_2\, i_l)(i_2\, i_{l-1}) \cdots (i_2\, i_3).$$

置换 σ 的两种写法包含相同个数 $l-1$ 个的不同的对换 (仅仅 $(i_1\ \ i_2) = (i_2\ \ i_1)$). 此外, 这些对换不是可交换的, 而它们的个数也不是一成不变的. 例如在 S_4 中

$$(1\ 2\ 3) = (1\ \ 3)(1\ \ 2) = (2\ \ 3)(1\ \ 3) = (1\ \ 3)(2\ \ 4)(1\ \ 2)(1\ \ 4).$$

3. 置换的符号 给出下述重要定理:

定理 2 设 π 是 S_n 中的一个置换, 将 π 分解成对换的乘积:

$$\pi = \tau_1 \tau_2 \cdots \tau_k, \tag{6}$$

称

$$\varepsilon_\pi = (-1)^k \tag{7}$$

为 π 的符号 (亦称符号差或奇偶性), 它由置换 π 唯一确定并不依赖于 (6) 式的分解方法, 即对于给定的 π , 整数 k 给出的奇偶性永远是唯一的. 此外任取 $\alpha, \beta \in S_n$,

$$\varepsilon_{\alpha\beta} = \varepsilon_\alpha \varepsilon_\beta. \tag{8}$$

证明 1) 设除 (6) 式外, 我们还有一个分解

$$\pi = \tau_1' \tau_2' \cdots \tau_{k'}', \tag{6'}$$

并且数 k 与 k' 是不同的. 定理的结论等价于说，整数 $k+k'$ 是一个偶数. 因为 $(\tau_s')^2=e$, 且 (6) 与 (6′) 给出 $\tau_1\tau_2\cdots\tau_k=\tau_1'\tau_2'\cdots\tau_{k'}'$, 用 $\tau_{k'}',\cdots,\tau_2',\tau_1'$ 从右侧顺序去乘这一等式的两边，我们得到 $\tau_1\tau_2\cdots\tau_k\tau_{k'}'\cdots\tau_2'\tau_1'=e$. 我们的问题可以归结成：设

$$e=\sigma_1\sigma_2\cdots\sigma_{m-1}\sigma_m\ ,\ m>0, \tag{9}$$

是单位置换到对换乘积的一个分解. 则 m 是一个偶数.

这个目的可以用下述方法实现: 将 e 的表达式 (9) 转化成 $m-2$ 个对换的乘积. 继续这一过程，如果 m 是奇数，我们就得到了一个对换 τ . 但显然 $e\neq\tau$. 根据以上分析，我们只需给出将 m 个因子削减为 $m-2$ 个的依据.

2) 设 $s,1\leqslant s\leqslant n$, 是任意一个包含在对换 $\sigma_2,\cdots,\sigma_m$ 中的整数. 为确定起见，设

$$e=\sigma_1\cdots\sigma_{p-1}\sigma_p\sigma_{p+1}\cdots\sigma_m,$$

使得 $\sigma_p=(s\ t)$, 而 $\sigma_{p+1},\cdots,\sigma_m$ 不包含 s. 对于 σ_{p-1}, 有下述四种可能性:

a) $\sigma_{p-1}=(s\ t)$; 这时 $\sigma_{p-1}\sigma_p=(s\ t)(s\ t)$ 从 e 的写法中排除，我们得到了 $m-2$ 个对换的分解式;

b) $\sigma_{p-1}=(s\ r),r\neq s,t$; 则

$$\sigma_{p-1}\sigma_p=(s\ r)(s\ t)=(s\ t)(r\ t),$$

于是我们将 s 向左移动了一个位置，对换的个数 m 没有改变;

c) $\sigma_{p-1}=(t\ r),r\neq s,t$; 则

$$\sigma_{p-1}\sigma_p=(t\ r)(s\ t)=(s\ r)(t\ r),$$

再次出现 b) 的情况， s 向左位移而对换的个数 m 没有改变;

d) $\sigma_{p-1}=(q\ r),\{q,r\}\cap\{s,t\}=\varnothing$; 这时

$$\sigma_{p-1}\sigma_p=(q\ r)(s\ t)=(s\ t)(q\ r).$$

如果出现情况 a), 我们的目的就达到了. 否则，不断重复 b)–d) 的处理方式，可以将 s 移动到左边第一个位置. 归根到底，我们或者有情况 a), 或者到达下述极限情况: $e=\sigma_1'\sigma_2'\cdots\sigma_m'$, $\sigma_1'=(s\ t')$, 且 s 不进入 $\sigma_2',\cdots,\sigma_m'$. 于是，当 $k>1$ 时 $\sigma_k'(s)=s$, 但 $s=e(s)=\sigma_1'(s)=t'\neq s$. 这个矛盾证明了情况 a) 必须出现，从而 m 是偶数，所以关于 ε_π 不变性的论断是正确的.

3) 如果 $\alpha=\tau_1\cdots\tau_k,\beta=\tau_{k+1}\cdots\tau_{k+l}$, 则 $\alpha\beta=\tau_1\cdots\tau_k\tau_{k+1}\cdots\tau_{k+l}$, 且 $\varepsilon_\alpha=(-1)^k,\varepsilon_\beta=(-1)^l$,$\varepsilon_{\alpha\beta}=(-1)^{k+l}=(-1)^k(-1)^l=\varepsilon_\alpha\varepsilon_\beta$. □

定义 若 $\varepsilon_\pi=1$, 则称置换 $\pi\in S_n$ 为 **偶置换**, 若 $\varepsilon_\pi=-1$, 则 π 为 **奇置换**. 根据定义，所有的对换都是奇置换，而 $\varepsilon_e=1$.

推论 设置换 $\pi \in S_n$ 分解为长为 $l_1, l_2, \cdots, l_m$ 的互不相交的循环的乘积. 则

$$\varepsilon_\pi = (-1)^{\sum\limits_{k=1}^{m}(l_k-1)}.$$

证明 事实上，根据定理 2, 我们有

$$\varepsilon_\pi = \varepsilon_{\pi_1\cdots\pi_m} = \varepsilon_{\pi_1}\cdots\varepsilon_{\pi_m}$$

其中，$\varepsilon_{\pi_k} = (-1)^{l_k-1}$，因为 π_k 可以写成 $l_k - 1$ 个对换的乘积 (见前述定理 1 的推论的证明). 最后

$$\varepsilon_\pi = (-1)^{l_1-1}\cdots(-1)^{l_m-1} = (-1)^{\sum\limits_{l=1}^{m}(l_k-1)}. \qquad \square$$

例 设 $\pi = \begin{pmatrix} 1\,2\,3\,4\,5\,6\,7\,8\,9\,10\,11 \\ 5\,4\,6\,7\,2\,9\,1\,3\,8\,11\,10 \end{pmatrix}$. 则 $\pi = (1\ 5\ 2\ 4\ 7)(3\ 6\ 9\ 8)(10\ 11)$，从 $l_1 = 5, l_2 = 4, l_3 = 2$ 得到 $\varepsilon_\pi = (-1)^{4+3+1} = 1$.

将 S_n 写成并集 $S_n = A_n \cup \bar{A}_n$, 其中

$$A_n = \{\pi \in S_n \,|\varepsilon_\pi = 1\}$$

是偶置换的集合，$\bar{A} = S_n \backslash A_n$ 是奇置换的集合. 设 $\tau = (i\ j)$ 是任意对换. S_n 到自身的映射 $L_\tau : \pi \mapsto \tau\,\pi$ 是一个一一映射. (L_τ 是单射：$\tau\alpha = \tau\beta \Rightarrow \alpha = \beta$；结论由 §5 定理 3 给出. 不难看出 L_τ^2 是恒等映射，故 $L_\tau^{-1} = L_\tau$). L_τ 可以直观地表示成在集合 $S_n = \{\pi_1 = e, \pi_2, \pi_3, \cdots, \pi_N\}$ 上的一个 $N = n!$ 阶置换：

$$L_\tau = \begin{pmatrix} \pi_1 & \pi_2 & \pi_3 & \cdots & \pi_N \\ \tau\pi_1 & \tau\pi_2 & \tau\pi_3 & \cdots & \tau\pi_N \end{pmatrix}. \tag{10}$$

类似地

$$R_\tau = \begin{pmatrix} \pi_1 & \pi_2 & \pi_3 & \cdots & \pi_N \\ \pi_1\tau & \pi_2\tau & \pi_3\tau & \cdots & \pi_N\tau \end{pmatrix} \tag{10$'$}$$

也是 S_n 上的一个置换. 映射 (10) 和 (10$'$) 以后会有更广泛的应用. 此刻我们指出 $\varepsilon_{\tau\pi} = \varepsilon_\tau\varepsilon_\pi = -\varepsilon_\pi$，所以

$$L_\tau(A_n) = \bar{A}_n, \quad L_\tau(\bar{A}_n) = A_n.$$

也就是说，S_n 中偶置换的个数等于奇置换的个数，从而

$$|A_n| = \frac{1}{2}\,|S_n| = \frac{n!}{2}. \tag{11}$$

4. S_n 在函数上的作用 S_n 中任一置换 σ 的符号的重要意义可以在计算 σ 逆序数时看到 (见本节最后的习题 5). 但现在不去管它，我们运用斜对称函数的概念，给出定理 2 的另一种证明，**斜对称函数** 本身也是重要且有用的.

定义 设 $\pi \in S_n$,f 是 n 个自变量的函数. 令

$$(\pi \circ f)(x_1, x_2, \cdots, x_n) = f(x_{\pi(1)}, \cdots, x_{\pi(n)}), \tag{12}$$

则称函数 $g = \pi \circ f$ 是由 π 作用在 f 上得到的.

引理 1 设 α,β 是 S_n 的任意置换. 则

$$(\alpha\beta) \circ f = \alpha \circ (\beta \circ f).$$

证明 根据公式 (12), 我们有

$$(\alpha \circ (\beta \circ f))(x_1, \cdots, x_n) = (\beta \circ f)(x_{\alpha(1)}, \cdots, x_{\alpha(n)}),$$

令 $y_k = x_{\alpha(k)}$, 并注意到 $y_{\beta(i)} = x_{\alpha(\beta(i))}$,

$$\begin{aligned}
&(\alpha \circ (\beta \circ f))(x_1, \cdots, x_n) = (\beta \circ f)(y_1, \cdots, y_n) \\
&= f(y_{\beta(1)}, \cdots, y_{\beta(m)}) = f(x_{\alpha(\beta(1))}, \cdots, x_{\alpha(\beta(n))}) \\
&= f(x_{(\alpha\beta)(1)}, \cdots, x_{(\alpha\beta)(n)}) = ((\alpha\beta) \circ f)(x_1, \cdots, x_n).
\end{aligned}$$ □

定义 一个 n 元函数 f 叫作 **斜对称的**, 若 $f(\cdots, x_k, x_{k+1}, \cdots) = -f(\cdots, x_{k+1}, x_k, \cdots)$, 也就是说, 当交换任意两个相邻变量的位置时, 函数值变号.

引理 2 交换任意两个变量的位置, 斜对称函数变号.

证明 设交换第 i,j 个自变量的位置, 且 $i < j$. 对位于 i,j 之间的自变量的个数 $l = j - i - 1$ 作归纳. 当 $l = 0$ 时, 引理的条件符合斜对称函数的定义. 设引理对任意 $j - i - 1 < l$ 真. 则

$$f(\cdots, x_i, x_{i+1}, \cdots, x_{j-1}, x_j, \cdots) = -f(\cdots, x_{i+1}, x_i, \cdots, x_{j-1}, x_j, \cdots)$$

$$= f(\cdots, x_{i+1}, x_j, \cdots, x_{j-1}, x_i, \cdots) = -f(\cdots, x_j, x_{i+1}, \cdots, x_{j-1}, x_i, \cdots).$$ □

应该指出, 并非所有的斜对称函数恒等于零. 下面是一个最简单的例子.

例 设

$$\Delta_n = \Delta_n(x_1, x_2, \cdots, x_n) = \prod_{1<j<i\leqslant n} (x_i - x_j)$$

符号 Π 表示乘积, 正如 Σ 表示求和. 指出任意两个相邻的自变量 x_k,x_{k+1}, 我们有 $\Delta_n = (x_{k+1} - x_k)[(x_{k+1} - x_{k-1}) \cdots (x_{k+1} - x_1)(x_k - x_{k-1}) \cdots (x_k - x_1)] \cdot A \cdot B$,
其中

$$A = \prod_{1\leqslant j<i<k} (x_i - x_j),$$

$$B = \prod_{s=k+2}^{n} [(x_s - x_{s-1}) \cdots (x_s - x_{k+1})\,(x_s - x_k) \cdots (x_s - x_1)].$$

交换 x_k 与 x_{k+1} 的位置，因子

$$[(x_{k+1}-x_{k-1})\cdots(x_{k+1}-x_1)\cdot(x_k-x_{k-1})\cdots(x_k-x_1)],$$

A 和 B 显然没有改变，可是

$$(x_k-x_{k+1})=-(x_{k+1}-x_k).$$

这就意味着

$$\Delta_n(\cdots,x_k,x_{k+1},\cdots)=-\Delta_n(\cdots,x_{k+1},x_k,\cdots),1\leqslant k\leqslant n+1.$$

Δ_n 是斜对称函数. 根据引理 2, 我们有

$$\Delta_n(\cdots,x_i,\cdots,x_j,\cdots)=-\Delta_n(\cdots,x_j,\cdots,x_i,\cdots).$$

此外，当 $x_1,\cdots,x_n$ 两两不同时，

$$\Delta_n(x_1,\cdots,x_n)\neq 0.$$

定理 2 的第二种证明 考虑任意 n 个变元 $x_1,\cdots,x_n$ 上的斜对称函数 f. 根据定理 1, 当置换 $\pi=\tau_1\tau_2\cdots\tau_k$ 分解成对换的乘积时， π 在 f 上的作用归结到对换 $\tau_k,\tau_{k-1},\cdots,\tau_1$ 在 f 上的逐次作用，即 k 个 (-1) 与 f 的乘积:

$$\pi\circ f=(\tau_1\cdots\tau_{k-1})\circ(\tau_k\circ f)=-(\tau_1\cdots\tau_{k-1})\circ f=\cdots=(-1)^k f=\varepsilon_\pi f.$$

因为这一关系式的左边依赖于 π，而不依赖于 π 的任何分解，所以由等式 (7) 指出的映射 ε: $\pi\mapsto\varepsilon_\pi$ 当 f 不是零函数时由置换 π 完全确定. 事实上，这样的函数是能够取到的，例如 $f=\Delta_n$.

按照引理 1 建立的法则将置换 $\alpha\beta$ 作用到这样的函数 f 上，

$$\begin{aligned}\varepsilon_{\alpha\beta}f=(\alpha\beta)\circ f=\alpha\circ(\beta\circ f)=\alpha\circ(\varepsilon_\beta f)=\varepsilon_\beta(\alpha\circ f)\\=\varepsilon_\beta(\varepsilon_\alpha f)=(\varepsilon_\beta\varepsilon_\alpha)f,\end{aligned}$$

从而得到关系式 (8). □

注记 我们将不止一次地研究 S_n 对函数的作用，在 [BA Ⅲ] 中可以看到这仅仅是一般规律的个别体现. 我们的另一个小小的成绩在于，将口头表达式 "在 $f(x_1,\cdots,x_n)$ 中交换 x_i 与 x_j 的位置", 简记作符号 $\tau\circ f$，其中 $\tau=(i\,j)$.

习 题

1. 在数学分析教科书中证明了斯特林公式

$$n!\sim\sqrt{2\pi n}\,n^n e^{-n},$$

此处 $e = 2.718281\cdots$ 是自然对数底，$\pi = 3.141592\cdots$；符号 $\sim$ 指当 $n \to \infty$ 时，$\sqrt{2\pi n}\ n^n e^{-n}/n!$ 趋近于 1. 借助阶乘公式检验近似估计 $100! > (9.33\cdots)10^{157}$. 在 S_{100} 中有多少长为 100 的循环？

2. 求置换 (4) 和置换

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 6 & 8 & 2 & 1 & 4 & 5 & 7 \end{pmatrix}$$

的阶.

3. 形如 (3) 的置换 π 含有 m 个互不相交的循环，令

$$m' = n - \sum_{k=1}^{m} l_k,$$

则 π 使 m' 个符号 (或点) 保持不变. 数 $d(\pi) = n - (m + m')$ 叫作置换 π 的**减量**. 验证 $\varepsilon_\pi = (-1)^{d(\pi)}$.

4. 计算置换

$$\pi = \begin{pmatrix} 1 & 2 & 3 & \cdots & n-1 & n \\ n & n-1 & n-2 & \cdots & 2 & 1 \end{pmatrix}$$

的符号.

5. 设 $\Omega = \{1, 2, \cdots, n\}$, $\Omega \times \Omega$ 是笛卡儿积. 称元素对 $(i\,j) \in \Omega \times \Omega$ 是置换 $\sigma \in S_n$ 的**逆序关系**(或简称 σ 逆序), 若 $i < j$, 但 $\sigma(i) > \sigma(j)$. 令

$$\operatorname{sgn}(\sigma) = \prod_{1 \leqslant i < j \leqslant n} \frac{\sigma(j) - \sigma(i)}{j - i}.$$

因为非零有理数 $(\sigma(j) - \sigma(i))/(j - i)$ 取负号. 当且仅当 $(i\,j)$ 是 σ 逆序，又因为 $\sigma : \Omega \to \Omega$ 是一一映射，所以 $\operatorname{sgn}(\sigma) = (-1)^k$, 其中 k 是 σ 逆序的总数. 易见

$$(\sigma(j)\sigma(i))\sigma = \begin{pmatrix} \cdots & \sigma(j) & \cdots & \sigma(i) & \cdots \\ \cdots & \sigma(i) & \cdots & \sigma(j) & \cdots \end{pmatrix} \begin{pmatrix} \cdots & i & \cdots & j \cdots & \\ \cdots & \sigma(i) & \cdots & \sigma(j) & \cdots \end{pmatrix}$$

$$= \begin{pmatrix} \cdots & i & \cdots & j & \cdots \\ \cdots & \sigma(j) & \cdots & \sigma(i) & \cdots \end{pmatrix}.$$

这样，σ 逆序 $(i\,j)$ 在作为置换 $\tau\sigma$ 的逆序时中止了，其中 $\tau = (\sigma(j), \sigma(i))$ 是一个对换.

证明可以找到 k 个对换 $\tau_1, \cdots, \tau_k$, 使得

$$\tau_k \tau_{k-1} \cdots \tau_1 \sigma = e,$$

其中 e 是单位置换. 则 $\sigma = \tau_1 \cdots \tau_{k-1}\tau_k$, 而 $\operatorname{sgn}\sigma = (-1)^k = \varepsilon_\sigma$, 这两种记号代表置换的同一个不变量；(从拉丁文 signum 引出的) 记号 sgn 就是符号的意思. 我们得到了另一种便利的方法来确定置换的符号 . 例如对应于置换 (4) 的逆序的集合由五个数对 (1 5),(2 5),(3 5),(4 5),(6 7) 组成，那么 $\operatorname{sgn}\pi = -1$. 事实上，事情归结为计算置换 π 的下面一行中比 i 大却位于 i 的前面的数字 j 的个数，$i = 1, 2, \cdots, n-1$.

§9 整数的算术

本节的目的是简述整数的初等可除性质，以便在后面的章节中引用. 进一步的结果将在第 5 章给出，在那里，整除性理论被推广到更一般的代数系统中.

1. 算术基本定理 若存在某个 $t \in \mathbb{Z}$, 使得 $n = st$, 则整数 s 叫作整数 n 的 **因数**(或 **因子**),n 本身叫作 s 的 **倍数**.n 被 s 整除记作 $s|n$, 而 n 不能被 s 整除记作 $s \nmid n$. 整除性是 $\mathbb{Z}$ 上的传递关系. 如果 $m|n$ 且 $n|m$, 则 $n = \pm m$, 而整数 n,m 叫作 **相伴的**. 如果整数 p 的全部因子为 $\pm p, \pm 1$(非真因子), 则称 p 为 **素数**. 通常约定素数是正的且大于 1.

下述定理表现出素数的基础作用.

算术基本定理 *每一个正整数 $n \neq 1$ 都可以分解成素数的乘积 $n = p_1p_2 \cdots p_s$. 这一写法除因子的次序外是唯一的.*

将相同因子收集到一起并改变记法，我们得到

$$n = p_1^{\varepsilon_1} p_2^{\varepsilon_2} \cdots p_k^{\varepsilon_k}, \quad \varepsilon_i > 0, \quad 1 \leqslant i \leqslant k.$$

任意有理数 $a = n/m \in \mathbb{Q}$ 也有类似的分解，但指数 ε_i 有正数也有负数.

我们指出，*全体素数的集合*

$$P = \{2, 3, 5, 7, 11, 13, \cdots\}$$

是 **无限集**(欧几里得定理). 事实上，如果仅有有限个素数，设为 $p_1, p_2, \cdots, p_t$, 那么根据基本定理，整数 $c = p_1p_2 \cdots p_t + 1$ 至少被某一个 p_i 除尽. 不失一般性，设 $c = p_1c'$. 则 $p_1(c' - p_2 \cdots p_t) = 1$, 这是不可能的，因为单位元在 $\mathbb{Z}$ 中的因子只有 ± 1. □

基本定理的证明将延迟至第 5 章给出. 一眼看来，定理似乎是显然的，以至不需要证明. 但事实并非如此，尽管所谈问题仅涉及整数乘法的性质 (整除性), 基本定理的证明却必须同时用到 $\mathbb{Z}$ 中的乘法和加法运算.

为了说明定理的非平凡性，考察 $\mathbb{N}$ 中的子集

$$S = \{4k + 1 | k = 0, 1, 2, \cdots\}.$$

S 关于乘法封闭：

$$(4k_1 + 1)(4k_2 + 1) = 4k_3 + 1.$$

对 $n \in S$ 作归纳不难证明分解的存在性 (类似于基本定理的第一部分), 即 n 可以分解成： $n = q_1 \cdots q_t$, 其中 q_i 不能用 S 中的元素做进一步分解. 称之为 **拟素数**. 5,9,13,17,21,49 都是这种拟素数的例子.

基本定理的第二部分对 S 不真，例如数 $441 \in S$ 就有两种不同的到拟素数的分解： $441 = 9 \cdot 49 = 21^2$.

2. $\mathbb{Z}$ 中的最大公约数和最小公倍数　如果允许使用零方幂 (永远认为 $p_i^0 = 1$), 任意两个整数 n 和 m 都可以写成同一组两两不等的素数方幂的乘积:

$$n = \pm p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}, \quad m = \pm p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}.$$

引入两个整数

$$\begin{aligned} \text{g.c.d}(n,m) &= p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_k^{\gamma_k}, \\ \text{l.c.m}(n,m) &= p_1^{\delta_1} p_2^{\delta_2} \cdots p_k^{\delta_k}, \end{aligned} \tag{1}$$

其中 $\gamma_i = \min\{\alpha_i, \beta_i\}$, $\delta_i = \max\{\alpha_i, \beta_i\}, i = 1, 2, \cdots, k$.

因为 $d|n \Rightarrow d = \pm p_1^{\alpha_1'} \cdots p_k^{\alpha_k'}, 0 \leqslant \alpha_i' \leqslant \alpha_i$, 所以从 (1) 式可得下述论断.

i) $\text{g.c.d}(n,m)|n$, $\text{g.c.d}(n,m)|m$, 并且若 $d|n, d|m$, 则 $d|\text{g.c.m}(n,m)$.

ii) $n|\text{l.c.m}(n.m)$, $m|\text{l.c.m}(n.m)$, 并且若 $n|u, m|u$, 则 $\text{l.c.m}(n,m)|u$.

性质 i) 和 ii) 证实了记号 g.c.d 和 l.c.m 分别是整数 n, m 的最大公因数和最小公倍数. 当 $n > 0$, $m > 0$ 时, 它们满足关系

$$\text{g.c.d}(n,m) \cdot \text{l.c.m}(n,m) = nm. \tag{2}$$

若 $\text{g.c.d}(n,m) = 1$, 则称整数 n, m 为 **互素的**. 这时 (2) 式具有形式 $\text{l.c.m}(n,m) = nm$.

3. $\mathbb{Z}$ 中的带余除法　给定 $a, b \in \mathbb{Z}, b > 0$, 总可以找到 $q, r \in \mathbb{Z}$, 使得

$$a = bq + r, \quad 0 \leqslant r < b$$

(如果仅仅假设 $b \neq 0$, 那么有不等式 $0 \leqslant r < |b|$).

证明　事实上, 集合

$$S = \{a - bs | s \in \mathbb{Z}, a - bs \geqslant 0\}$$

显然不空 (例如 $a - b(-a^2) > 0$). 于是 S 包含一个最小元素, 记作 $r = a - bq$. 根据条件, $r \geqslant 0$. 假如 $r \geqslant b$, 我们得到元素 $r - b = a - b(q+1) \in S$, 它小于 r . 这一矛盾说明, r 必须小于 b. □

上述简单的论证给出了一个 **算法**, 可以通过有限步找到 **商数** q 和 **余数** r, $\mathbb{Z}$ 中的带余除法可以用来给出 g.c.d 的另一种定义, 如果注意到关系式 (2), 还有 l.c.m 的另一种定义.

作法如下, 给定不全为零的整数 n 和 m, 令

$$J = \{nu + mv | u, v \in \mathbb{Z}\} \tag{3}$$

选出 J 中的最小正数 $d = nu_0 + mv_0$. 运用带余除法将 n 写作 $n = dq + r, 0 \leqslant r < d$. 我们有

$$r = n - dq = n - (nu_0 + mv_0)q = n(1 - u_0 q) + m(-v_0 q) \in J,$$

从 d 的选取得到 $r=0$. 因而 $d|n$. 类似地， $d|m$. 现在假设 d' 是数 n 和 m 的任意一个公因子. 这时

$$d'|n, d'|m \Rightarrow d'|nu_0, d'|mv_0 \Rightarrow d'|(nu_0+mv_0) \Rightarrow d'|d.$$

这样 d 具备最大公因数的一切性质，所以 $d=\text{g.c.d}(n,m)$. 我们证明了下述论断.

命题 两个不全为零的整数的最大公因数总可以写成下述形式：

$$\text{g.c.d}(n,m)=nu+mv, \qquad u,v\in\mathbb{Z} \tag{4}$$

特别地，整数 n,m 互素，当且仅当存在某对 $u,v\in\mathbb{Z}$, 使得

$$nu+mv=1. \tag{4'}$$

证明 我们已经验证过，互素的整数 n,m 满足关系式 (4'). 反之，如果 n,m 满足 (4'), 则

$$d|n, d|m \Rightarrow d|nu, d|mv \Rightarrow d|(nu+mv) \Rightarrow d|1 \Rightarrow d=\pm1. \qquad \square$$

关系式 (4) 和 (4') 的证明是非常有用的. 只需从集合 J 中取出任意一个正数 (见 (3) 式), 然后借助带余除法找到 J 中越来越小的正数，直到得出最小的正数，这就是最大公因数.

习 题

1. 每一个不等于 2 的素数都可以写成 $4k+1$ 或 $4k-1$ 的形式. 运用在第 1 段给出的集合 S 的乘法证明，形如 $4k-1$ 的素数有无穷多个.

2. 下述论断是非平凡的.

若 $n,m\in\mathbb{Z}$, $\text{g.c.d}(n,m)=1$, 如果 p 是整除 n^2+m^2 的一个素数，则 $p=4k+1$.

试用该论断证明存在无穷多个形如 $4k+1$ 的素数.

3. 如果自然数 n 恰可被 r 个不同的素数 $p_1,\cdots,p_r$ 整除，则小于 n 且与 n 互素的整数的个数

$$\varphi(n)=n(1-\frac{1}{p_1})\cdots(1-\frac{1}{p_r}).$$

函数 $\varphi:\mathbb{N}\to\mathbb{N}$ 叫作**欧拉函数**.

证明公式当 $n\leqslant 25$ 时，以及当 $n=p^m$ 时成立.

4. 运用二项式定理，对 n 作归纳证明，若 p 是素数，则 n^p-n 对任意 $n\in\mathbb{Z}$ 可以被 p 整除 .

第 2 章　矩　阵

在第一章 §3 中介绍的长方矩阵是如此常见，以至于随着时间的推移产生了数学的一个独立的分支 ——矩阵论. 矩阵论是在 19 世纪中叶建立起来的，稍后与线性代数的发展同步，逐渐得到了完善和精确. 到目前为止，矩阵论仍然是重要的研究工具，既适合于实际应用，又适合于现代数学的抽象结构. 我们将在本章给出矩阵论最简要的结果.

矩阵是向量空间的线性映射的自然伴侣. 在线性代数与几何教程中 [BA Ⅱ], 我们将赋予这一论断精确的含义. 在本章中，空间，向量，线性相关性，方程组的秩等概念将从纯代数的方面展开，以满足我们直接目标的需要.

§1　行和列的向量空间

1. 问题的提出　由于线性方程组，我们研究了含义各不相同的长为 n 的行. 它们是 $m\times n$ 矩阵 $A=(a_{ij})$ 的行 $(a_{i1},a_{i2},\cdots,a_{in}),1\leqslant i\leqslant n$, 以及系数矩阵为 A 的线性方程组的解 ($x_1^0,x_2^0,\cdots,x_n^0$). 在第 1 章 §3, 把一个线性方程组或矩阵化为阶梯形时，除 (I) 型初等变换外运用了两种重要的运算：将一行乘以一个常数并加到另一行上. 对于 **齐次** 线性方程组的解也可以施行这两种运算. 事实上，如果 $(x_1',x_2',\cdots,x_n')$ 和 $(x_1'',x_2'',\cdots,x_n''$) 是线性方程组

$$a_{i1}x_1+a_{i2}x_2+\cdots+a_{in}x_n=0,\quad i=1,2,\cdots,m$$

的两个解， α,β 是任意两个实数，则行

$$(\alpha x_1'+\beta x_1'',\alpha x_2'+\beta x_2'',\cdots,\alpha x_n'+\beta x_n'')$$

也是我们的方程组的解:

$$
\begin{aligned}
&a_{i1}(\alpha x_1' + \beta x_1'') + a_{i2}(\alpha x_2' + \beta x_2'') + \cdots + a_{in}(\alpha x_n' + \beta x_n'') \\
&= \alpha(a_{i1}x_1' + a_{i2}x_2' + \cdots + a_{in}x_n') + \beta(a_{i1}x_1'' + a_{i2}x_2'' + \cdots + a_{in}x_n'') = 0
\end{aligned}
$$

另一方面,任意的行,无论它代表什么,都是一般集合 $\mathbb{R}^n$ 中的一个元素,其中 $\mathbb{R}^n$ 是实数集 $\mathbb{R}$ 的 n 次笛卡儿幂. 所以我们希望去研究这种一般的对象,然后将其性质自然地运用到矩阵和齐次线性方程组的解上.

2. 基本定义 设 n 是一个固定的自然数. $\mathbb{R}$ 上长为 n 的 *行向量空间* 指集合 $\mathbb{R}^n$(其元素称为 **行向量** 或简称 **向量**), 连同向量的加法运算以及 **纯量** (实数) 与向量的乘法运算. 纯量用小写拉丁字母或希腊字母表示,而向量像矩阵一样用大写拉丁字母表示. 事实上,向量 $X = (x_1, x_2, \cdots, x_n)$ 可以看成一个 $1 \times n$ 矩阵. 设 $Y = (y_1, y_2, \cdots, y_n)$ 也是一个向量, λ 是纯量. 根据定义

$$
\begin{aligned}
&X + Y = (x_1 + y_1, x_2 + y_2, \cdots, x_n + y_n), \\
&\lambda X = (\lambda x_1, \lambda x_2, \cdots, \lambda x_n).
\end{aligned}
$$

零向量 (0,0,⋯,0) 今后用一般的符号 0 表示. 此外 $\mathbb{R}^1$ 显然与 $\mathbb{R}$ 恒同.

读者熟知的实数的运算法则无条件地适用于 $\mathbb{R}^n$. 尽管列举它们是枯燥的,但给出它们的精确定义,有助于理解 *抽象的向量空间*, 我们将在后面的线性代数和几何课程中学习这种向量空间.

VS_1 : $X + Y = Y + X$ 对任意向量 $X,Y \in \mathbb{R}^n$ 成立 (交换律);

VS_2 : $(X + Y) + Z = X + (Y + Z)$ 对任意三个向量 $X, Y, Z \in \mathbb{R}^n$ 成立 (结合律);

VS_3 : 存在一个特别的 (零) 向量 0, 使得 $X + 0 = X$ 对所有的 $X \in \mathbb{R}^n$ 成立;

VS_4 : 每个向量 $X \in \mathbb{R}^n$ 对应一个负向量 $-X$, 使得 $X + (-X) = 0$;

VS_5 : $1X = X$ 对所有的 $X \in \mathbb{R}^n$ 成立;

VS_6 : $(\alpha\beta)X = \alpha(\beta X)$ 对所有的 $\alpha, \beta \in \mathbb{R}, X \in \mathbb{R}^n$ 成立;

VS_7 : $(\alpha + \beta)X = \alpha X + \beta X$;

VS_8 : $\alpha(X + Y) = \alpha X + \alpha Y$.

在 VS_3 和 VS_4 中向量 0 及 $-X$ 的唯一性是所列法则的简单推论 (如果考虑抽象的向量空间则是公理), 我们不做推导,而将它们看作明显的事实.

术语 "向量"(或 *线性*) 空间的起源在第一学期的解析几何课程中已有说明,在那里建立了笛卡儿平面的点 (向量) 与它们的坐标 (x, y) 之间的一一对应. 由平行四边形法则给出的向量的加法和用数去乘向量恰好对应于 $\mathbb{R}^2$ 中向量的运算.

除了长为 n 的行向量空间外，也可以考虑高为 n 的列向量组成的向量空间

$$\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = [x_1, x_2, \cdots, x_n],$$

列向量表示成我们在第 1 章 §3 中约定的样子. 显然，行空间和列空间之间的区别纯属约定，但我们很快就会看到，给出空间的这两种形式是有益处的. 一般来说，我们从上下文就可以判断考虑的是行空间还是列空间，所以不引进任何特别的记号来加以区分.

3. 线性组合. 线性包 设 $X_1, X_2, \cdots, X_k$ 是向量空间 $\mathbb{R}^n$ 中的向量，$\alpha_1, \alpha_2, \cdots, \alpha_k$ 是纯量. 向量 $X = \alpha_1 X_1 + \alpha_2 X_2 + \cdots + \alpha_k X_k$ 叫作向量 X_i 的带有系数 α_i 的**线性组合**. 例如，

$(2,3,5,5) - 3(1,1,1,1) + 2(1,0,-1,-1) = (1,0,0,0)$.

其次设 $Y = \beta_1 X_1 + \beta_2 X_2 + \cdots + \beta_k X_k$ 是同样的向量 X_i 带有系数 β_i 的线性组合，而 $\alpha, \beta \in \mathbb{R}$. 则

$$\begin{aligned} \alpha X + \beta Y &= \alpha(\alpha_1 X_1 + \alpha_2 X_2 + \cdots + \alpha_k X_k) \\ &\quad + \beta(\beta_1 X_1 + \beta_2 X_2 + \cdots + \beta_k X_k) \\ &= (\alpha\alpha_1 + \beta\beta_1) X_1 + (\alpha\alpha_2 + \beta\beta_2) X_2 \\ &\quad + \cdots + (\alpha\alpha_k + \beta\beta_k) X_k \end{aligned}$$

也是向量 x_i 的线性组合，其系数为 $\alpha\alpha_i + \beta\beta_i$. 于是我们看到，由给定向量组 $X_1, X_2, \cdots, X_k$ 的所有线性组合构成的集合 V 具有性质

$$X, Y \in V \Rightarrow \alpha X + \beta Y \in V \tag{1}$$

对所有的 $\alpha, \beta \in \mathbb{R}$ 成立. 特别地，零向量永远包含在 V 中.

V 通常用符号 $\langle X_1, X_2, \cdots, X_k \rangle$ 表示，并称之为向量组 $X_1, X_2, \cdots, X_k$ 的**线性包**(或简称 **包**). 通常称包 $\langle X_1, X_2, \cdots, X_k \rangle$ 是在 $X_1, X_2, \cdots, X_k$ 上**张成的**, 或称由向量 $X_1, X_2, \cdots, X_k$**生成的**.

可以定义任意子集 $S \subset \mathbb{R}^n$ 的线性包 $\langle S \rangle$,$\langle S \rangle$ 是 S 中的任意 有限 个向量的任意线性组合构成的集合. 显然，如果 V 是 $\mathbb{R}^n$ 中的一个线性包，则 $\langle V \rangle = V$: V 当中向量的任意线性组合仍属于 V. 特别地， $S \subset V \Rightarrow \langle S \rangle \subset V$, 也就是说线性包 $\langle S \rangle$ 可以定义成 $\mathbb{R}^n$ 中包有 S 的任意向量的集合的线性包的交：

$$\langle S \rangle = \bigcap_{S \subset V} V. \tag{2}$$

初看起来结论并不明显，需要验证 (2) 式右边线性包的交集还是一个线性包. 事实上如果 $X, Y \in \cap V$ 那么对于这个集合中的每一个 $V, X, Y \in V$. 这就意味着

$\alpha X+\beta Y\in V$ 对所有的 $\alpha,\beta\in\mathbb{R}$ 成立，从而给出了所需的包含关系 $\alpha X+\beta Y\in\cap V$. 与交不同，两个线性包 U 和 V 的并 $U\cup V$ 一般来说不是一个线性包，例如在 $\mathbb{R}^2$ 中，$U=\{(\lambda,0)|\lambda\in\mathbb{R}\},V=\{(0,\lambda)|\lambda\in\mathbb{R}\}$.

例 1 设

$$U_m=\{(\lambda_1,\cdots,\lambda_m,0,\cdots,0)|\ \lambda_i\in\mathbb{R}\}\subset\mathbb{R}^n,$$
$$V_m=\{(0,\cdots,0,\lambda_{m+1},\cdots,\lambda_n)|\ \lambda_i\in\mathbb{R}\}\subset\mathbb{R}^n,$$

$0<m<n$. 直接验证可知 U_m,V_m 都是线性包, 并且 $\langle U_m,\ V_m\rangle=\mathbb{R}^n$，$U_m\cap V_m=\{0\}$.

例 2 在空间 $\mathbb{R}^n$ 中考察 **单位行向量**

$$E_{(1)}=(1,\ 0,\ \cdots,\ 0),\ \ E_{(2)}=(0,\ 1,\ \cdots,\ 0),\ \cdots,\ E_{(n)}=(0,\ 0,\ \cdots,\ 1).\tag{3}$$

每一个向量 $X=(x_1,\ x_2,\ \cdots,\ x_n)$ 可唯一地表示成 $X=x_1E_{(1)}+x_2E_{(2)}+\cdots+x_nE_{(n)}$. 所以

$$\mathbb{R}^n=\langle E_{(1)},\ E_{(2)},\ \cdots,\ E_{(n)}\rangle.$$

单位列向量 将记作

$$E^{(1)}=[1,\ 0,\ \cdots,\ 0],\ \ E^{(2)}=[0,\ 1,\ \cdots,\ 0],\ \cdots,\ E^{(n)}=[0,\ 0,\ \cdots,\ 1].\tag{3$'$}$$

4. 线性相关性　空间 $\mathbb{R}^n$ 的向量组 $X_1,\ \cdots,\ X_k$ 称为 **线性相关的**, 如果可以找到 k 个不全为零的数 $\alpha_1,\ \cdots,\ \alpha_k$, 使得

$$\alpha_1X_1+\alpha_2X_2+\cdots+\alpha_kX_k=0\tag{4}$$

(右边是零向量). 并称线性式 (4) 为非平凡的. 如果 $\alpha_1X_1+\alpha_2X_2+\cdots+\alpha_kX_k=0\Rightarrow\alpha_1=\alpha_2=\cdots=\alpha_k=0$, 则向量 $X_1,\ X_2,\ \cdots,\ X_k$ 叫作 **线性无关的**.

第 3 段例 2 表明，单位向量 $E_{(1)},\ E_{(2)},\ \cdots,\ E_{(n)}$ 是线性无关的. 一个向量 $X\neq 0$ 显然总是线性无关的，因为 $(\lambda X=0,\ X\neq 0)\Rightarrow\lambda=0$. 其次，$X_1,\ \cdots,X_k$ 是线性无关的这一性质与向量的顺序无关，因为 (4) 式中的项 α_iX_i 可以用任意顺序排列.

定理 1 下述论断成立:

i) 如果向量组 $\{X_1,\ \cdots,\ X_k\}$ 的某一个部分组是线性相关的，则向量组本身也是线性相关的.

ii) 线性无关的向量组 $\{X_1,\ \cdots,\ X_k\}$ 的任意部分组都是线性无关的.

iii) 在线性相关的向量 $X_1,\ \cdots,\ X_k$ 中间，至少有一个向量是其余向量的线性组合.

iv) 如果向量 $X_1,\ \cdots,\ X_k$ 中间有一个向量是其余向量的线性组合，则向量 $X_1,\ \cdots,\ X_k$ 是线性相关的.

v) 如果向量 $X_1, \cdots, X_k$ 线性无关，而 $X_1, \cdots, X_k, X$ 线性相关，则 X 是向量 $X_1, \cdots, X_k$ 的线性组合.

vi) 如果向量 $X_1, \cdots, X_k$ 是线性无关的，而向量 X_{k+1} 不能表示成它们的线性组合，则向量组 $\{X_1, \cdots, X_k, X_{k+1}\}$ 是线性无关的.

证明 i) 设前 s 个向量 $X_1, \cdots, X_s$, $s<k$, 是线性相关的，即存在不全为零的 α_i, 使得

$$\alpha_1 X_1 + \cdots + \alpha_s X_s = 0.$$

令 $\alpha_{s+1} = \cdots = \alpha_k = 0$, 我们得到一个非平凡关系

$$\alpha_1 X_1 + \cdots + \alpha_s X_s + \alpha_{s+1} X_{s+1} + \cdots + \alpha_k X_k = 0.$$

论断 ii) 从 i) 立即得出 (用反证法).

iii) 不失一般性，设在关系式 (4) 中 $\alpha_k \neq 0$. 则

$$X_k = -\frac{\alpha_1}{\alpha_k} X_1 - \cdots - \frac{\alpha_{k-1}}{\alpha_k} X_k.$$

iv) 设 $X_k = \beta_1 X_1 + \cdots + \beta_{k-1} X_{k-1}$. 令 $\alpha_1 = \beta_1, \cdots, \alpha_{k-1} = \beta_{k-1}, \alpha_k = -1$, 得到关系式 (4), 且系数 $\alpha_k \neq 0$.

v) 如果有非平凡的关系式

$$\beta_1 X_1 + \cdots + \beta_k X_k + \beta X = 0$$

使得 $\beta \neq 0$, 则 X 是 $X_1, \cdots, X_k$ 的线性组合. 若 $\beta = 0$, 则由 $X_1, \cdots, X_k$ 线性无关的条件，知 $\beta_1 = \cdots = \beta_k = 0$, 与关系式的非平凡性矛盾.

论断 vi) 由 v) 立即得出. □

5. 基. 维数 我们现在给出一个重要的

定义 设 V 是 $\mathbb{R}^n$ 中的一个非零线性包. 向量组 $X_1, \cdots, X_r \in V$ 称为 V 的**基**, 如果它们是线性无关的，且它们生成的线性包与 V 重合:

$$\langle X_1, \cdots, X_k \rangle = V.$$

从基和向量组的线性包的定义推出，每一个向量 $X \in V$ 都可以唯一地写成 $X = \alpha_1 X_1 + \cdots + \alpha_k X_k$ 的形式. 系数 $\alpha_1, \cdots, \alpha_k \in \mathbb{R}$ 叫作 X 相对于基 $X_1, \cdots, X_k$ 的 **坐标**.

正如我们已经看到的, 线性无关的单位向量 (3) 生成 $\mathbb{R}^n$. 于是, $\{E_{(1)}, E_{(2)}, \cdots, E_{(n)}\}$ 成为向量空间 $\mathbb{R}^n$ 的基，称之为 **标准基**. 但它不是 $\mathbb{R}^n$ 中唯一的基. 例如

$$E'_{(1)} = E_{(1)},\ E'_{(2)} = E_{(1)} + E_{(2)},\ E'_{(3)} = E_{(1)} + E_{(2)} + E_{(3)},\ \cdots$$

$$E'_{(n)} = E_{(1)} + E_{(2)} + \cdots + E_{(n)}$$

也是空间 $\mathbb{R}^n$ 的基 (仔细验证). 另一方面，直到现在尚未明确，是否 $\mathbb{R}^n$ 中的每一个线性包都有一组基，如果有，基向量的个数是否不变. 这两个问题的回答都是肯定的. 我们的论证基于下述引理.

引理 *设 V 是 $\mathbb{R}^n$ 中的一个以 $X_1, \cdots, X_r$ 为基的线性包. 而 $Y_1, Y_2, \cdots, Y_s$ 是 V 中一个线性无关的向量组. 则 $s \leqslant r$.*

证明 就像 V 中所有的向量一样， $Y_1, \cdots, Y_s$ 是基向量的线性组合. 设

$$
\begin{aligned}
Y_1 &= a_{11}X_1 + a_{21}X_2 + \cdots + a_{r1}X_r,\\
Y_2 &= a_{12}X_1 + a_{22}X_2 + \cdots + a_{r2}X_r,\\
&\cdots\cdots\cdots\cdots\\
Y_s &= a_{1s}X_1 + a_{2s}X_2 + \cdots + \alpha_{rs}X_r,
\end{aligned}
$$

其中 a_{ij} 是纯量 (是唯一确定的向量 Y_j 的坐标，但后一点目前对我们并不重要).

用反证法. 假设 $s > r$. 写出 Y_j 的以 x_j 为系数的线性组合：

$$
\begin{aligned}
x_1Y_1 + \cdots + x_sY_s = (a_{11}x_1 + a_{12}x_2 + \cdots + a_{1s}x_s)X_1 + \cdots\\
+(a_{r1}x_1 + a_{r2}x_2 + \cdots + a_{rs}x_s)X_r,
\end{aligned}
$$

并考察含有 r 个方程， s 个未知数的线性方程组

$$
\begin{aligned}
a_{11}x_1 + a_{12}x_2 + \cdots + a_{1s}x_s &= 0,\\
\cdots\cdots\cdots\cdots\\
a_{r1}x_1 + a_{r2}x_2 + \cdots + a_{rs}x_s &= 0.
\end{aligned}
$$

因为假设 $s > r$, 根据第 1 章 §3 推论 2, 我们的方程组有非零解 $(x_1^0, \cdots, x_s^0)$. 我们得到了一个非平凡的线性关系

$$
x_1^0Y_1 + x_2^0Y_2 + \cdots + x_s^0Y_s = 0,
$$

与引理的条件矛盾. 这就意味着 $s \leqslant r$. □

定理 2 *$\mathbb{R}^n$中的每一个非零线性包 $V \subset \mathbb{R}^n$ 都有一组有限基. 线性包 V 的所有的基都含有相同个数的向量. 这个个数 $r \leqslant n$, 称 r 为线性包 V 的维数, 记作 $\dim_{\mathbb{R}} V$ 或简记作 $\dim V$.*

证明 根据条件， V 包含有至少一个非零向量 X_1(行或列). 设我们已在 V 中找到了一个线性无关的向量组 $\{X_1, \cdots, X_k\}$. 如果线性包 $\langle X_1, \cdots, X_k\rangle$ 不等于 V, 那么我们在 V 中选出一个向量 $X_{k+1} \notin \langle X_1, \cdots, X_k\rangle$. 换言之， X_{k+1} 不是 $X_1, \cdots, X_k$ 的线性组合. 根据定理 1, vi), 向量组 $\{X_1, \cdots, X_k, X_{k+1}\}$ 是线性无关的. 这一扩充线性无关向量组的过程可以无限制地继续下去，但是所有的向量都在 $\mathbb{R}^n = \langle E_{(1)}, E_{(2)}, \cdots, E_{(n)}\rangle$ 中，而引理证明了， $\mathbb{R}^n$ 中任意的线性无关组最多包含有 n 个向量. 因而对于某个自然数 $r \leqslant n$, 线性无关组 $X_1, \cdots, X_k, \cdots, X_r \in V$

成为 **极大的**, 即任取 V 中的向量 $X \neq 0$, 向量组 $\{X_1, \cdots, X_r, X\}$ 是线性相关的. 由定理 1,v), 有 $X \in \langle X_1, \cdots, X_r\rangle$. 所以 $V = \langle X_1, \cdots, X_r\rangle$, 而向量 $X_1, \cdots, X_r$ 构成 V 的一组基.

现在设 $Y_1, \cdots, Y_s$ 也是 V 的一组基. 根据引理, 我们有不等式 $s \leqslant r$. 交换 $X_1, \cdots, X_r$ 与 $Y_1, \cdots, Y_s$ 的位置, 再一次由引理得到不等式 $r \leqslant s$. 因此 $s = r$, 定理得证. □

尽管不太必要, 我们还是指出, 上述所有的讨论既适合于行空间, 也适合于列空间.

这样, $\mathbb{R}^n$ 中的每一个非零线性包 V 都具有一个正整数 $r \leqslant n$, 称之为维数 $r = \dim V$. 特别地 $\dim \mathbb{R}^n = n$. 向量空间的这一重要参数也可以用其他的方法进行刻画. 维数另一种可能的定义基于向量组秩的概念. 即如果 $\{X_1, X_2, \cdots\}$ 是 $\mathbb{R}^n$ 中的一个向量组 (可能是无限的), 则如我们所知道的, 线性包 $\langle x_1, \cdots\rangle$ 的维数不超过 n . 这一维数叫作向量组 $\{X_1, X_2, \cdots\}$ 的 **秩**:

$$\operatorname{rank}\{X_1, X_2, \cdots\} = \dim\langle X_1, X_2, \cdots\rangle.$$

当 $V = \{0\}$ 时, 显然可以认为 $\dim V = 0$.

习 题

1.① 设 U 和 V 是 $\mathbb{R}^n$ 中的两个线性包, 线性包 $\langle U \cup V\rangle$ 叫作 U 与 V 的 **和**:

$$U + V = \langle U \cup V\rangle = \{u + v | u \in U, v \in V\}$$

如果 $U \cap V = 0$, 则称 $U + V$ 为 **直和**, 记作 $U \oplus V$.

设 $V = V_1 \oplus V_2$, 且 $X = X_1 + X_2 = X_1' + X_2'$ 是向量 $X \in V$ 的两种线性组合, 此处 $X_1, X_1' \in V_1, X_2, X_2' \in V_2$, 则有 $X_1 - X_1' = X_2' - X_2 \in V_1 \cap V_2$, 因为 $V_1 \cap V_2 = 0$, 所以 $X_1 = X_1', X_2 = X_2'$.

证明逆命题: 如果对于每一个向量 $X \in V$, 写法 $X = X_1 + X_2$ 都是唯一的, 此处 $X_i \in V_i$, 则和式 $V = V_1 + V_2$ 是直和. 更一般地, 如果 $V_1, \cdots, V_k$ 是 $\mathbb{R}^n$ 中的线性包, 并且对于每一个向量 $X \in V$, 表法 $X = X_1 + \cdots + X_k$ 都是唯一的, 此处 $X_i \in V_i$, 则称 $V = V_1 \oplus \cdots \oplus V_k$ 为 **直和**.

2. 设 V, V_1 和 V_2 都是 $\mathbb{R}^n$ 中的线性包, 并且 $V \subset V_1 + V_2$. 等式 $V = V \cap V_1 + V \cap V_2$ 永远成立吗? 在 $V_1 \subset V$ 的特殊情况下, 这一关系式成立吗?

3. 设 V 是 $\mathbb{R}^n$ 中的一个线性包. 如果 $V = U \oplus W$ 是一个直和分解, 则 W 叫作 U 在 V 中的一个 **补**. 而 U 叫作 W 在 V 中的一个 **补**. U 在 V 中的补是唯一确定的吗? 试比较 W 与集合论概念下的补集 $V \backslash U$ (见 §5 第 1 段).

4. 证明向量 $X_1 = (1, 2, 3)$, $X_2 = (3, 2, 1)$ 是线性无关的, 考察线性包 $V = \langle X_1, X_2\rangle$; 证明向量 $X = (-5, 2, 9)$ 属于 V, 并计算 X 在基 X_1, X_2 下的系数; 求 V 在 $\mathbb{R}^3$ 中的任意一个补.

---

①原著中设 U 和 V 是两个子空间, 但此处子空间的定义尚未给出. —— 译者注.

5. 证明，$\mathbb{R}^n$ 中的向量组 $X_1, \cdots, X_n$ 张成 $\mathbb{R}^n$，当且仅当它们是线性无关的.

6. 设 V 是 $\mathbb{R}^n$ 的一个线性包，证明 V 中任意线性无关的向量 $X_1, \cdots, X_k$ 可以扩充成 V 的一组基.

7. 设 U 和 V 是 $\mathbb{R}^n$ 中的线性包. 证明若 $U \cap V = 0$, 则 $\dim(U+V) = \dim U + \dim V$.

8. 计算向量组 (0, 1, 1), (1, 0, 1), (1, 1, 0) 的秩.

§2 矩阵的秩

1. 方程组的回顾 在高为 m 的列向量空间 $\mathbb{R}^m$ 中，考察 n 个向量

$$A^{(j)} = [a_{1j}, a_{2j}, \cdots, a_{mj}],\ j = 1, 2, \cdots, n,$$

以及它们的线性包 $V = \langle A^{(1)}, A^{(2)}, \cdots, A^{(n)} \rangle$. 假设再给出一个向量 B，问 B 是否在线性包 $V \subset \mathbb{R}^m$ 中，如果在，它的坐标 $b_1, \cdots, b_m$(在 §1(3′) 的标准基下) 是怎样通过 $A^{(j)}$ 的坐标表示出来的. 当 $\dim V = n$ 时，问题的第二部分相当于确定向量 B 在基 $A^{(1)}, \cdots, A^{(n)}$ 之下的坐标. 为此，我们取 $A^{(j)}$ 以未知数 x_j 为系数的线性组合，并构造方程 $x_1A^{(1)} + \cdots + x_nA^{(n)} = B$. 该方程的直观形式为

$$x_1\begin{pmatrix} a_{11} \\ a_{21} \\ \vdots \\ a_{m1} \end{pmatrix} + x_2\begin{pmatrix} a_{12} \\ a_{22} \\ \vdots \\ a_{m2} \end{pmatrix} + \cdots + x_n\begin{pmatrix} a_{1n} \\ a_{2n} \\ \vdots \\ a_{mn} \end{pmatrix} = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{pmatrix}. \tag{1}$$

方程的另一种写法是含有 m 个方程，n 个未知数的线性方程组

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n &= b_1, \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n &= b_2, \\ \cdots\cdots\cdots\cdots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n &= b_m. \end{aligned} \tag{2}$$

这就是我们最初在第 1 章 §3 中遇到过的方程组. 在那里我们引入了线性方程组 (2) 的系数矩阵[①] 和 增广矩阵.

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix},$$

①原书为 “矩阵”, 此处按惯例译作 “系数矩阵”.—— 译者注.

$$(A|B) = \left(\begin{array}{cccc|c} a_{11} & a_{12} & \cdots & a_{1n} & b_1 \\ a_{21} & a_{22} & \cdots & a_{2n} & b_2 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} & b_m \end{array} \right). \tag{3}$$

乍一看来，我们又回到了出发点，浪费了时间而什么都没得到．但事实上，我们现在得到了一系列重要的概念．余下的事情是学会使用它们．

先来约定一些符号．我们通常将和 $s_1+s_2+\cdots+s_n$ 简写成 $\sum\limits_{i=1}^{n} s_i$．此处 $s_1, \cdots, s_n$ 是满足数或向量的加法法则的任意量 (数，行向量等等)．法则

$$\sum_{i=1}^{n} ts_i = t\sum_{i=1}^{n} s_i \ , \quad \sum_{i=1}^{n}(s_i+t_i) = \sum_{i=1}^{n} s_i + \sum_{i=1}^{n} t_i$$

是不证自明的．

我们也要考虑下述 **双重和**

$$\sum_{j=1}^{n}\sum_{i=1}^{m} a_{ij} = \sum_{j=1}^{n}\left(\sum_{i=1}^{m} a_{ij}\right) = \sum_{i=1}^{m}\left(\sum_{j=1}^{n} a_{ij}\right) = \sum_{i,j} a_{ij},$$

求和的顺序 (按照第一或第二个脚标) 可以根据自己的希望选择．易见，如果将 a_{ij} 排成 $m\times n$ 阶的长方阵，那么矩阵元素的求和既可以按行进行，也可以按列进行．

其他可能的求和类型将在需要时介绍．

2. 矩阵的秩 上节引入的线性包 $V = \langle A^{(1)}, A^{(2)}, \cdots, A^{(n)}\rangle$ 叫作 $m\times n$ 阶长方阵 A (见公式 (3)) 的 **列空间**．将 V 记作 $V_c(A)$ 或简记作 V_c (其中 c 表示列)．维数 $r_c(A) = \dim V_c$ 叫作矩阵 A 的 **列秩**．类似地可定义矩阵 A 的 **行秩**:$r_r(A) = \dim V_r$，此处 $V_r = \langle A_{(1)}, A_{(2)}, \cdots, A_{(m)}\rangle$ 是矩阵 A 的 **行空间**，即由 $\mathbb{R}^n$ 中的行向量 $A_{(i)} = (a_{i1}, a_{i2}, \cdots, a_{in})$, $i = 1, 2, \cdots, m$, 生成的线性包 (其中 r 表示行)．换言之，

$$r_c(A) = \mathrm{rank}\{A^{(1)}, A^{(2)}, \cdots, A^{(n)}\},$$
$$r_r(A) = \mathrm{rank}\{A_{(1)}, A_{(2)}, \cdots, A_{(m)}\}$$

分别为行向量组和列向量组的秩．根据 §1 定理 2, 数值 $r_c(A)$ 和 $r_r(A)$ 的定义是合理的．

按照第 1 章 §3 的术语，称矩阵 A' 是由矩阵 A 经过 I 型初等变换得到的，如果有某对脚标 $s\neq t$，使得 $A'_{(s)} = A_t$, $A'_{(t)} = A_s$，但对任意脚标 $i\neq s, t$, $A'_{(i)} = A_{(i)}$；称矩阵 A' 是由矩阵 A 经过 II型初等变换 得到的，如果有某对脚标 $s\neq t$，使得任取脚标 $i\neq s$, $A'_{(i)} = A_{(i)}$，而 $A'_s = A_{(s)} + \lambda A_{(t)}$，其中 $\lambda\in\mathbb{R}$. 注意到初等变换是在 A 的行上进行的．

我们指出，两类初等变换都是可逆的，也就是说，从 A 得到的矩阵 A' 可以借助于初等变换重新变回到 A，并且所用的初等变换是同型的．

引理 如果矩阵 A' 是由长方阵 A 经过有限多次初等行变换得到的，则有等式

i) $r_{\mathrm{r}}(A') = r_{\mathrm{r}}(A)$;

ii) $r_{\mathrm{c}}(A') = r_{\mathrm{c}}(A)$.

证明 只要考虑 A' 是由 A 经过一次初等行变换得到的情况就足够了.

i) 因为

$$\langle A_{(1)}, \cdots, A_{(s)}, \cdots, A_{(t)}, \cdots, A_{(m)}\rangle = \langle A_{(1)}, \cdots, A_{(t)}, \cdots, A_{(s)}, \cdots, A_{(m)}\rangle,$$

所以 I 型初等变换不改变 $r_{\mathrm{r}}(A)$. 另一方面，

$$A'_{(s)} = A_{(s)} + \lambda A_{(t)} \Rightarrow A_{(s)} = A'_{(s)} - \lambda A_{(t)},$$

从而

$$\begin{aligned} &\langle A_{(1)}, \cdots, A_{(s)} + \lambda A_{(t)}, \cdots, A_{(t)}, \cdots, A_{(m)}\rangle \\ =& \langle A_{(1)}, \cdots, A_{(s)}, \cdots, A_{(t)}, \cdots, A_{(m)}\rangle, \end{aligned}$$

这样 II 型初等变换也不改变 $r_{\mathrm{r}}(A)$.

ii) 设 $A'^{(j)}, 1 \leqslant j \leqslant n$，是矩阵 A' 的列. 我们来证明

$$\sum_{j=1}^{n} \lambda_j A^{(j)} = 0 \Leftrightarrow \sum_{j=1}^{n} \lambda_j A'^{(j)} = 0. \tag{4}$$

为此，考察 A 和 A' 对应的齐次线性方程组 HLS 和 HLS′，它们用 (1) 的形式给出 (常数项取零):

$$\text{HLS}: \ \sum_{j=1}^{n} x_j A^{(j)} = 0 \ , \ \ \text{HLS}': \sum_{j=1}^{n} x_j A'^{(j)} = 0.$$

矩阵 A 与 A' 的关系使得 HLS′ 是由 HLS 经过 I 型或 II 型初等变换得到的. 根据第 1 章 §3 定理 1,HLS 与 HLS′ 等价，即一个方程组的所有的解 $(\lambda_1, \lambda_2, \cdots, \lambda_n)$ 也是另一个的解，这样，蕴含关系 (4) 成立.

综上所述，一个矩阵的列向量的极大线性无关组的向量个数与另一个矩阵列向量的相应个数相符，这就确立了等式 $r_{\mathrm{c}}(A') = r_{\mathrm{c}}(A)$. □

本节的基本结论是下述断言.

定理 1 对于任意 $m \times n$ 阶长方阵 A, 等式 $r_{\mathrm{c}}(A) = r_{\mathrm{r}}(A)$ 成立 (这个数叫作矩阵 A 的秩，记作 $\operatorname{rank} A$).

证明 根据第 1 章 §3 定理 2, 经过有限次初等行变换，矩阵 A 可以化成阶梯形

$$
\bar{A} = \begin{pmatrix}
\bar{a}_{11} & \cdots & \bar{a}_{1k} & \cdots & \bar{a}_{1l} & \cdots & \bar{a}_{1s} & \cdots & \bar{a}_{1n} \\
0 & \cdots & \bar{a}_{2k} & \cdots & \bar{a}_{2l} & \cdots & \bar{a}_{2s} & \cdots & \bar{a}_{2n} \\
0 & \cdots & 0 & \cdots & \bar{a}_{3l} & \cdots & \bar{a}_{3s} & \cdots & \bar{a}_{3n} \\
\cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\
0 & \cdots & 0 & \cdots & 0 & \cdots & \bar{a}_{rs} & \cdots & \bar{a}_{rn} \\
0 & \cdots & 0 & \cdots & 0 & \cdots & 0 & \cdots & 0 \\
\cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\
0 & \cdots & 0 & \cdots & 0 & \cdots & 0 & \cdots & 0
\end{pmatrix} \tag{5}
$$

其中 $\bar{a}_{11}\cdot\bar{a}_{2k}\cdot\bar{a}_{3l}\cdots\bar{a}_{rs}\neq 0$，根据引理

$$r_{\mathrm{c}}(A)=r_{\mathrm{c}}(\bar{A}),\quad r_{\mathrm{r}}(A)=r_{\mathrm{r}}(\bar{A}),$$

我们只需证明等式 $r_{\mathrm{c}}(\bar{A})=r_{\mathrm{r}}(\bar{A})$ 就足够了.

在矩阵 A 与 $\bar{A}$ 中脚标为 1, k, l, $\cdots$, s 的列叫作列向量基. 它们对应于线性方程组 (2) 的主未知数 x_1, x_k, $x_l,\cdots$, x_s. 列向量基这一术语是很有道理的. 假设矩阵 (5) 的第 1, k, l, $\cdots$, s 个列向量

$$
\begin{gathered}
\bar{A}^{(1)}=[\bar{a}_{11},\ 0,\ \cdots,\ 0],\ \bar{A}^{(k)}=[\bar{a}_{1k},\ \bar{a}_{2k},\ 0,\cdots,\ 0],\cdots \\
\cdots,\ \bar{A}^{(s)}=[\bar{a}_{1s},\ \bar{a}_{2s},\ \cdots,\ \bar{a}_{rs},\ 0,\ \cdots,\ 0],
\end{gathered}
$$

如果它们之间有关系式

$$\lambda_1\bar{A}^{(1)}+\lambda_k\bar{A}^{(k)}+\lambda_l\bar{A}^{(l)}+\cdots+\lambda_s\bar{A}^{(s)}=0,$$

则

$$\lambda_s\bar{a}_{rs}=0,\quad \cdots,\quad \lambda_l\bar{a}_{3l}=0,\quad \lambda_k\bar{a}_{2k}=0,\quad \lambda_1\bar{a}_{11}=0,$$

又因为 $\bar{a}_{11}\cdot\bar{a}_{2k}\cdot\bar{a}_{3l}\cdots\bar{a}_{rs}\neq 0$，故 $\lambda_1=\lambda_k=\lambda_l=\lambda_s=0$. 于是

$$
\begin{gathered}
\operatorname{rank}\{\bar{A}^{(1)},\ \bar{A}^{(k)},\ \bar{A}^{(l)},\ \cdots,\ \bar{A}^{(s)}\}=r, \\
r_{\mathrm{c}}(\bar{A})\geqslant r.
\end{gathered}
$$

但是矩阵 $\bar{A}$ 的列空间 $\bar{V}_{\mathrm{c}}$ 等同于从 $\bar{A}$ 中删去后 $m-r$ 个零行所成矩阵的列空间. 所以

$$r_{\mathrm{c}}(\bar{A})=\dim\bar{V}_{\mathrm{c}}\leqslant\dim\mathbb{R}^r=r.$$

比较两个不等式得到 $r_{\mathrm{c}}(\bar{A})=r$. (不等式 $r_{\mathrm{c}}(\bar{A})\leqslant r$ 也可以从一个显然的事实得到，即矩阵 $\bar{A}$ 的所有的列都是列向量基的线性组合；我们把这一论断留作习题.)

另一方面，矩阵 $\bar{A}$ 的所有非零行是线性无关的：任意线性关系

$$\lambda_1\bar{A}_{(1)}+\lambda_2\bar{A}_{(2)}+\cdots+\lambda_r\bar{A}_{(r)}=0,\quad \lambda_i\in\mathbb{R}$$

如同在列向量的情况一样，给出

$$\lambda_1\bar{a}_{11}=0,\ \lambda_2\bar{a}_{2k}=0,\ \cdots,\ \lambda_r\bar{a}_{rs}=0,$$

因而 $\lambda_1=\lambda_2=\cdots=\lambda_r=0$. 于是 $r_{\mathrm{r}}(\bar{A})=r=r_{\mathrm{c}}(\bar{A})$. □

3. 可解性准则 矩阵 A 的阶梯形可以回答对应的线性方程组 (见第 1 章 §3) 的一系列问题，但阶梯形依赖于初等变换的实施过程，例如，列向量基，或等价地方程组 (2) 中的主未知数，可以有不同的选择. 尽管如此，我们却可以从定理 1 及其证明得出下述

推论 *若 $b_1=b_2=\cdots=b_m=0$，则齐次线性方程组 (2) 中主未知数的个数不依赖于化为阶梯形的方式，它等于 $\mathrm{rank}\,A$，其中 A 是方程组的系数矩阵.*

证明 我们已经看到，主未知数的个数等于矩阵 $\bar{A}$ (见公式 (5)) 的非零行的个数，后者等于矩阵 A 的秩. 而矩阵的秩是唯一确定的. (这句话表明，矩阵的秩作为它的内在特征，不依赖于任何外加状况.) □

在下一章中，我们将得到一个有效的方法去计算矩阵 A 的秩，不需要将 A 化为阶梯型. 无疑地这将使基于秩概念的一系列论断提高价值. 这种论断的一个简单而有用的例子是第 1 章中谈到的线性方程组的可解性准则.

定理 2(*克罗内克 – 卡皮里*) *线性方程组 (2) 是可解的，当且仅当它的系数矩阵的秩等于增广矩阵的秩 (见 (3)).*

证明 将线性方程组 (2) 写成形式 (1)，它的可解性可以解释成下述问题 (见本节开头)：列向量 B 是否可以表示成矩阵 A 的列向量的线性组合. 如果 B 能这样表示 (即方程组 (2) 是可解的)，则 $B\in\langle A^{(1)},\ \cdots,\ A^{(n)}\rangle$，那么 $\mathrm{rank}\{A^{(1)},\ \cdots,\ A^{(n)}\}=\mathrm{rank}\{A^{(1)},\ \cdots,\ A^{(n)},\ B\}$，于是 $\mathrm{rank}\ A=r_{\mathrm{c}}(A)=r_{\mathrm{c}}((A|B))=\mathrm{rank}(A|B)$ (见定理1).

反之，如果矩阵 A 与矩阵 $(A|B)$ 有相同的秩，且 $\{A^{(j_1)},\cdots,A^{(j_r)}\}$ 是矩阵 A 列向量组的极大线性无关组，则扩张组 $\{A^{(j_1)},\ \cdots,\ A^{(j_r)},\ B\}$ 是线性相关的，根据 §1 定理 1,v),B 是基本列 $A^{(j)}$ 的线性组合. 于是方程组 (2) 是可解的. □

习 题

1. 不把 $m\times n$ 阶矩阵 $A=(a_{ij})$ 化成阶梯形，证明定理 1.

提示：设 $\dim V_{\mathrm{r}}(A)=r,\ \dim V_{\mathrm{c}}(A)=s$. 选择 r 个基行；不失一般性，可以假定它们是前 r 行 $A_{(1)},\ A_{(2)},\ \cdots,\ A_{(r)}$. 考察由 A 的前 r 行组成的 $r\times n$ 矩阵 $\tilde{A}=[A_{(1)},\ A_{(2)},\ \cdots,\ A_{(r)}]$. 在 $\tilde{A}$ 中选择 t 个基列，此处 $t=\dim V_{\mathrm{c}}(\tilde{A})$. 设为 $\tilde{A}^{(1)},\ \cdots,\ \tilde{A}^{(t)}$. 因为 $V_{\mathrm{c}}(\tilde{A})\subset\mathbb{R}^r$，故 $t\leqslant r$. 对于 A 的任意列 $A^{(k)},\ k>t$，可以找到常数 $\lambda_1,\ \cdots,\ \lambda_t\in\mathbb{R}$，使得 $A^{(k)}=\lambda_1A^{(1)}+\cdots+\lambda_tA^{(t)}$，即 $a_{ik}=\sum_{p=1}^{t}\lambda_pa_{ip},\ 1\leqslant i\leqslant m$. 当 $i\leqslant r$ 时，这是显然的，因为我们有关于 $\tilde{A}$ 列的关系式 $\tilde{A}^{(k)}=\lambda_1\tilde{A}^{(1)}+\cdots+\lambda_t\tilde{A}^{(t)}$. 当 $i>r$ 时，运用第 i 行通过前 r 列的表达式 $A_{(i)}=\mu_1A_{(1)}+\cdots+\mu_rA_{(r)}$，得到

$$a_{ik}=\sum_{l=1}^{r}\mu_l a_{lk}=\sum_{l=1}^{r}\mu_l\sum_{p=1}^{t}\lambda_p a_{lp}=\sum_{p=1}^{t}\lambda_p\sum_{l=1}^{r}\mu_l a_{lp}=\sum_{p=1}^{t}\lambda_p a_{ip}.$$

列的线性相关性准则表明，$s\leqslant t$, 但上述证明给出 $t\leqslant r$, 故 $s\leqslant r$. 进一步，考察 $n\times m$ 阶转置矩阵

$$^tA=\begin{pmatrix} a_{11} & a_{21} & \cdots & a_{m1}\\ a_{12} & a_{22} & \cdots & a_{m2}\\ \cdots & \cdots & \cdots & \cdots\\ a_{1n} & a_{2n} & \cdots & a_{mn}\end{pmatrix}$$

得到等式 $r_r(^tA)=r_c(A)$, $r_c(^tA)=r_r(A)$，所以根据上述证明 $r\leqslant s$. 综上所述，$r=s$.

2. 如同行的情况，交换矩阵 A 的第 s 列和第 t 列，叫作 I 型初等变换，而将第 t 列乘以常数 λ 加到第 s 列上，叫作 II 型初等变换.

描述矩阵 A 经初等列变换化成的阶梯形. 用初等列变换将矩阵 $\bar{A}$(见公式 (5)) 化为形式

$$\tilde{A}=\left(\begin{array}{cccc|ccc} \tilde{a}_{11} & & & & & & \\ & \tilde{a}_{22} & & & & & \\ & & \ddots & & & & \\ & & & \tilde{a}_{rr} & & & \\ \hline & & & & 0 & & \\ & & & & & \ddots & \\ & & & & & & 0 \end{array}\right),$$

其中

$$\tilde{a}_{11}=\bar{a}_{11},\ \tilde{a}_{22}=\bar{a}_{2k},\ \tilde{a}_{33}=\bar{a}_{3l},\cdots,\tilde{a}_{rr}=\bar{a}_{rs};\prod_{i=1}^{r}\tilde{a}_{ii}\neq 0.$$ [①]

3. 证明若 $a_0\neq 0$, 方阵

$$A=\begin{pmatrix} 0 & 0 & \cdots & 0 & 0 & a_0\\ 1 & 0 & \cdots & 0 & 0 & a_1\\ 0 & 1 & \cdots & 0 & 0 & a_2\\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots\\ 0 & 0 & \cdots & 1 & 0 & a_{n-2}\\ 0 & 0 & \cdots & 0 & 1 & a_{n-1}\end{pmatrix}$$

的秩为 n.

4. 设两个矩阵

$$A=\begin{pmatrix} \alpha_1 & \alpha_2 & \cdots & \alpha_n\\ \beta_1 & \beta_2 & \cdots & \beta_n\end{pmatrix},\quad B=\begin{pmatrix} \alpha_1 & \alpha_2 & \cdots & \alpha_n\\ \beta_1 & \beta_2 & \cdots & \beta_n\\ \gamma_1 & \gamma_2 & \cdots & \gamma_n\end{pmatrix}$$

---

① $\tilde{A}$ 是一个 $m\times n$ 矩阵，不能写成 $\mathrm{diag}(\tilde{a}_{11},\tilde{a}_{22},\cdots,\tilde{a}_{rr},0,\cdots,0)$.—— 译者注.

试用平面上 n 条直线所成集合的几何性质给出 A 和 B 有相等秩的条件.

§3 线性映射. 矩阵的运算

1. 矩阵和映射 设 $\mathbb{R}^n$ 和 $\mathbb{R}^m$ 分别为高为 n, m 的列向量空间. 设 $A=(a_{ij})$ 是一个 $m\times n$ 阶矩阵. 定义一个映射 $\varphi_A:\mathbb{R}^n\to\mathbb{R}^m$, 将任意向量 $X=[x_1,x_2,\cdots,x_n]\in\mathbb{R}^n$, 对应到

$$\varphi_A(X)=x_1A^{(1)}+x_2A^{(2)}+\cdots+x_nA^{(n)}. \tag{1}$$

其中 $A^{(1)},\cdots,A^{(n)}$ 是矩阵 A 的列 (与 §2(1) 相比较). 由于它们的高是 m ,(1) 式的右边给出了一个列向量 $Y=[y_1,\ y_2,\ \cdots,\ y_m]\in\mathbb{R}^m$. 更详尽地, (1) 式可写成如下形式

$$y_i=\sum_{j=1}^n a_{ij}x_j\ ,\ \ i=1,\ 2,\ \cdots,\ m. \tag{1'}$$

如果 $X=X'+X''=[x_1'+x_1'',\ x_2'+x_2'',\ \cdots,\ x_n'+x_n'']$, 则

$$\begin{aligned}\varphi_A(X'+X'')&=\sum_{i=1}^n(x_i'+x_i'')A^{(i)}=\sum_{i=1}^n x_i'A^{(i)}+\sum_{i=1}^n x_i''A^{(i)}\\&=\varphi_A(X')+\varphi_A(X'').\end{aligned}$$

类似地,

$$\varphi_A(\lambda X)=\sum_{i=1}^n\lambda x_iA^{(i)}=\lambda\sum_{i=1}^n x_iA^{(i)}=\lambda\varphi_A(X),\ \lambda\in\mathbb{R}.$$

反之, 设 $\varphi:\mathbb{R}^n\to\mathbb{R}^m$ 是第 1 章 §5 意义下的映射, 具有下述两条性质:

i) $\varphi(X'+X'')=\varphi(X')+\varphi(X''),\quad\forall\,X',\ X''\in\ \mathbb{R}^n$;

ii) $\varphi(\lambda X)=\lambda\varphi(X),\quad\forall X\in\mathbb{R}^n,\ \lambda\in\mathbb{R}$.

我们知道 (见 §1 第 3 段),$\mathbb{R}^n=\langle E^{(1)},\cdots,E^{(n)}\rangle$ 是列向量的标准基的线性包, 则

$$X=[x_1,\ x_2,\ \cdots,\ x_n]=\sum_{j=1}^n x_jE^{(j)}.$$

运用性质 i),ii) 得到

$$\varphi(X)=\varphi\left(\sum_{j=1}^n x_jE^{(j)}\right)=\sum_{j=1}^n x_j\varphi(E^{(j)}). \tag{2}$$

关系式 (2) 表明, 映射 φ 由它在列向量基上的取值完全确定. 令

$$\varphi(E^{(j)})=[a_{1j},\ a_{2j},\ \cdots,\ a_{mj}]=A^{(j)}\in\mathbb{R}^m, \tag{3}$$

我们发现，给出 φ 等价于给出列为 $A^{(1)}, \cdots, A^{(n)}$ 的 $m\times n$ 阶长方阵 $A=(a_{ij})$. 关系式 (1) 和 (2) 实质上是一致的. 我们可以写 $\varphi=\varphi_A$.

定义 满足性质 i),ii) 的映射 $\varphi=\varphi_A\colon\mathbb{R}^n\to\mathbb{R}^m$ 叫作从 $\mathbb{R}^n$ 到 $\mathbb{R}^m$ 的 **线性映射**. 特别地当 $m=n$ 时叫作 **线性变换**. 矩阵 A 叫作 **线性映射** φ_A **的矩阵**.

设 φ_A,$\varphi_{A'}$ 是 $\mathbb{R}^n\to\mathbb{R}^m$ 的两个线性映射，分别有矩阵 $A=(a_{ij})$ 和 $A'=(a'_{ij})$. 等式 $\varphi_A=\varphi_{A'}$ 成立，当且仅当任取 $X\in\mathbb{R}^n$, 值 $\varphi_A(X)=\varphi_{A'}(X)$. 特别地，

$$A'^{(j)}=\varphi_{A'}(E^{(j)})=\varphi_A(E^{(j)})=A^{(j)},\ 1\leqslant j\leqslant n,$$

所以 $a'_{ij}=a_{ij}$, 故 $A'=A$.

将我们的结果概括如下.

定理 1 从 $\mathbb{R}^n$ 到 $\mathbb{R}^m$ 的线性映射与 $m\times n$ 阶矩阵之间存在着一一对应.

这里强调指出，谈论任意集合 S 到 T 的线性映射 $S\to T$ 是没有意义的. 条件 i) 和 ii) 预先假定了 S 和 T 分别是 $\mathbb{R}^n$ 和 $\mathbb{R}^m$ 中的线性包.

我们注意到 $m=1$ 的特殊情况，这样的线性映射 $\varphi\colon\mathbb{R}^n\to\mathbb{R}$ 通常称为 n 变元**线性函数**, 由给定的 n 个纯量 $a_1, a_2, \cdots, a_n$ 给出:

$$\varphi(X)=\varphi(x_1,\ x_2,\ \cdots,\ x_n)=a_1x_1+a_2x_2+\cdots+a_nx_n. \tag{4}$$

注记 我们这里的线性函数和中学时的概念有所区别，那时的线性函数指 $x\mapsto ax+b$(只谈单变元 x 的情况).

线性函数 (4), 如同任意的线性映射: $\mathbb{R}^n\to\mathbb{R}^m$ 一样; 可以做加法和纯量乘法. 事实上，设 φ_A, $\varphi_B:\mathbb{R}^n\to\mathbb{R}^m$ 是两个线性映射. 映射

$$\varphi=\alpha\varphi_A+\beta\varphi_B\colon\mathbb{R}^n\to\mathbb{R}^m,\quad \alpha,\beta\in\mathbb{R}$$

在 X 上的取值定义为

$$\varphi(X)=\alpha\varphi_A(X)+\beta\varphi_B(X).$$

右边是通常的列向量的线性组合.

因为

$$\begin{aligned}
\varphi(X'+X'')&=\alpha\varphi_A(X'+X'')+\beta\varphi_B(X'+X'')\\
&=\alpha\{\varphi_A(X')+\varphi_A(X'')\}+\beta\{\varphi_B(X')+\varphi_B(X'')\}\\
&=\{\alpha\varphi_A(X')+\beta\varphi_B(X')\}+\{\alpha\varphi_A(X'')+\beta\varphi_B(X'')\}\\
&=\varphi(X')+\varphi(X'');\\
\varphi(\lambda X)&=\alpha\varphi_A(\lambda X)+\beta\varphi_B(\lambda X)=\alpha\lambda\varphi_A(X)+\beta\lambda\varphi_B(X)\\
&=\lambda\{\alpha\varphi_A(X)+\beta\varphi_B(X)\}=\lambda\varphi(X),
\end{aligned}$$

所以 φ 是一个线性映射 (在这里，我们未加说明地使用了 §1 的法则 $\mathrm{VS}_1-\mathrm{VS}_8$). 根据定理 1, 我们有线性变换的矩阵 C , 使得 $\varphi=\varphi_C$. 为了求出 C , 按照公式 (3) 写

出第 j 个列向量：

$$
\begin{aligned}
&[c_{1j}, c_{2j}, \cdots, c_{mj}] = C^{(j)} = \varphi_C(E_n^{(j)}) \\
&= \alpha\varphi_A(E_n^{(j)}) + \beta\varphi_B(E_n^{(j)}) = \alpha A^{(j)} + \beta B^{(j)} \\
&= [\alpha a_{1j} + \beta b_{1j}, \alpha a_{2j} + \beta b_{2j}, \cdots, \alpha a_{mj} + \beta b_{mj}].
\end{aligned}
$$

很自然地，将矩阵 $C = (c_{ij})$ ，其中元素 $c_{ij} = \alpha a_{ij} + \beta b_{ij}$ ，叫作矩阵 A 和 B 的以 α 和 β 为系数的线性组合：

$$
\begin{aligned}
&\alpha \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \cdots & \cdots & \cdots \\ a_{m1} & \cdots & a_{mn} \end{pmatrix} + \beta \begin{pmatrix} b_{11} & \cdots & b_{1n} \\ \cdots & \cdots & \cdots \\ b_{m1} & \cdots & b_{mn} \end{pmatrix} \\
&= \begin{pmatrix} \alpha a_{11} + \beta b_{11} & \cdots & \alpha a_{1n} + \beta b_{1n} \\ \cdots & \cdots & \cdots \\ \alpha a_{m1} + \beta b_{m1} & \cdots & \alpha a_{mn} + \beta b_{mn} \end{pmatrix}.
\end{aligned} \tag{5}
$$

于是

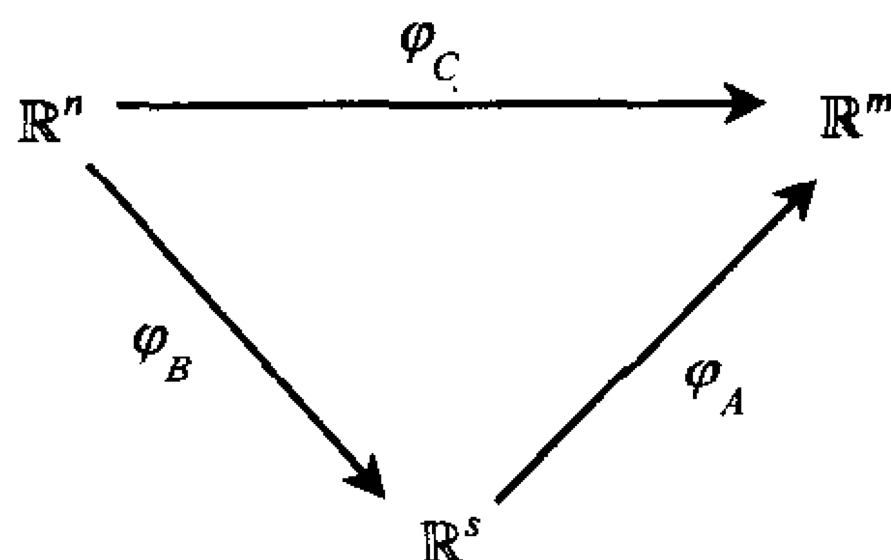
$$
\alpha\varphi_A + \beta\varphi_B = \varphi_{\alpha A + \beta B}. \tag{6}
$$

我们将经常运用下述事实：线性函数的线性组合也是一个线性函数.

最后，我们指出，如果把所有的行向量 X, Y, Z 换成 $m \times n$ 阶矩阵，对应的运算由公式 (5) 确定，并且将 §1 中对向量空间的法则 $\mathrm{VS}_1 - \mathrm{VS}_8$ 重写一遍，就得到了法则 $\mathrm{VSM}_1 - \mathrm{VSM}_8$, 因而我们可以定义 $m \times n$ 阶矩阵的向量空间. 如果方便，它也可看作是密集写法的长度为 $m \cdot n$ 的行向量空间 $\mathbb{R}^{m \cdot n}$(将行折断为长度为 n 的段，一个排在另一个的下面).

2. 矩阵的乘积 公式 (5) 和 (6) 给出了 $m \times n$ 矩阵的集合以及从 $\mathbb{R}^n$ 到 $\mathbb{R}^m$ 的线性变换的集合之间加法和数乘运算的一致性. 在考虑任意集合时，还有一个重要的运算概念，即映射的合成 (见第 1 章 §5, 第 2 段). 有理由期望，两个线性映射的合成应当与矩阵的合成方式一致. 我们来看如何做到这一点.

设 $\varphi_B: \mathbb{R}^n \to \mathbb{R}^s, \varphi_A: \mathbb{R}^s \to \mathbb{R}^m$ 是线性映射， $\varphi_C = \varphi_A \circ \varphi_B$ 是它们的合成：



一般来说，在把乘积 $\varphi = \varphi_A \circ \varphi_B$ 写成 φ_C 之前，需要验证 φ 是线性变换，这是很清楚的：

(i) $\varphi(X'+X'')=\varphi_A(\varphi_B(X'+X''))=\varphi_A(\varphi_B(X')+\varphi_B(X''))$
$=\varphi_A(\varphi_B(X'))+\varphi_A(\varphi_B(X''))=\varphi(X')+\varphi(X'')$;

(ii) $\varphi(\lambda X)=\varphi_A(\varphi_B(\lambda X))=\varphi_A(\lambda\varphi_B(X))=\lambda\varphi_A(\varphi_B(X))=\lambda\varphi(X)$;

所以根据定理 1,φ 由某个矩阵 C 完全确定.

假定映射在列上的作用为

$$[x_1,\cdots,x_n]\xrightarrow{\varphi_B}[y_1,\cdots,y_s]\xrightarrow{\varphi_A}[z_1,\cdots,z_m],$$

按照公式 (1′) 的显式表达:

$$z_i=\sum_{k=1}^{s}a_{ik}y_k=\sum_{k=1}^{s}a_{ik}\sum_{j=1}^{n}b_{kj}x_j=\sum_{j=1}^{n}\left(\sum_{k=1}^{s}a_{ik}b_{kj}\right)x_j.$$

另一方面,

$$z_i=\sum_{j=1}^{n}c_{ij}x_j,\qquad i=1,2,\cdots,m.$$

比较所得的表达式并注意到 x_j 是任意实数 $(j=1,2,\cdots,n)$, 我们得到

$$c_{ij}=\sum_{k=1}^{s}a_{ik}b_{kj},\qquad 1\leqslant i\leqslant m,\quad 1\leqslant j\leqslant n. \tag{7}$$

矩阵 $C=(c_{ij})$ 叫作矩阵 A乘以 矩阵 B 得到的结果. 记作

$$C=AB.$$

这样, 一个 $m\times s$ 阶长方阵 (a_{ik}) 与 $s\times n$ 阶长方阵 (b_{ki}) 的乘积是一个 $m\times n$ 阶长方阵 (c_{ij}), 其元素 c_{ij} 由公式 (7) 给出.

我们证明了

定理 2 由矩阵 A 和 B 确定的两个线性变换的乘积 $\varphi_A\cdot\varphi_B$ 是由矩阵 $C=AB$ 确定的线性变换. 换言之,

$$\varphi_A\varphi_B=\varphi_{AB}. \tag{8}$$

公式 (8) 是对公式 (6) 的自然的补充.

我们可以忘记线性变换去求任意两个矩阵 A 和 B 的乘积 AB, 但必须记住, 符号 AB 有意义, 当且仅当矩阵 A 的列数等于矩阵 B 的行数. 在这一条件下, 等式 (7) 给出了乘积的 (i,j) 元是 A 的第 i 行 $A_{(i)}$ 与 B 的第 j 列 $B^{(j)}$ 的乘积,

$$c_{ij}=(a_{i1},\cdots,a_{is})[b_{1j},\cdots,b_{sj}]=A_{(i)}B^{(j)}. \tag{9}$$

矩阵 AB 的行数等于矩阵 A 的行数, 而 AB 的列数等于矩阵 B 的列数. 特别地, 同阶方阵的乘积总是有定义的, 但即使在这种情况下, 一般来说, $AB\neq BA$,

例如：

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}=\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}\neq\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}=\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}.$$

当然还可以有许多其他的方式定义矩阵的乘积 (例如行与行相乘), 但是没有一种方式能够与上述定义的重要性相比. 这并不奇怪, 因为我们是通过映射的自然合成得到矩阵乘法的, 而映射当属现代数学最基本的概念.

推论 矩阵的乘法满足结合律：

$$A(BC)=(AB)C.$$

证明 矩阵的乘积对应于线性映射的乘积 (见定理 2 和公式 (8)), 根据第 1 章 §5 定理 1, 任意映射的乘积是结合的, 也可以根据公式 (7) 直接计算进行验证. □

再来看 **分配律**:

$$(A+B)C=AC+BC,\quad D(A+B)=DA+DB, \tag{10}$$

其中 A,B,C,D 分别是阶数为 $m\times s, m\times s, s\times n, n\times m$ 的任意矩阵.

事实上, 令 $A=(a_{ij}), B=(b_{ij}), C=(c_{ij})$, 对任意 i,j 有等式 (根据 $\mathbb{R}$ 的分配律)

$$\sum_{k=1}^{n}(a_{ik}+b_{ik})c_{kj}=\sum_{k=1}^{n}a_{ik}c_{ik}+\sum_{k=1}^{n}b_{ik}c_{kj},$$

左边给出了矩阵 $(A+B)C$ 的元素 g_{ij}, 而右边分别给出了 AC 的元素 h_{ij} 和 BC 的元素 h'_{ij}.(10) 中的第二个分配律法则可类似得到.

3. 矩阵的转置 阶数分别为 $m\times n$ 与 $n\times m$ 的两个矩阵

$$A=\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix},\qquad {}^tA=\begin{pmatrix} a_{11} & a_{21} & \cdots & a_{m1} \\ a_{12} & a_{22} & \cdots & a_{m2} \\ \cdots & \cdots & \cdots & \cdots \\ a_{1n} & a_{2n} & \cdots & a_{mn} \end{pmatrix}$$

叫作 **互为转置**, 其中的任意一个都是由另一个将行变为列, 列变为行得到的 (细心的读者会注意到, 转置的概念已经在 §2 第 1 段遇到过了). 易见

$${}^t({}^tA)=A,\quad {}^t(A+B)={}^tA+{}^tB,\quad {}^t(\lambda A)=\lambda\,{}^tA.$$

矩阵乘积的转置满足一个更有趣的规律. 如果

$$A=\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1s} \\ a_{21} & a_{22} & \cdots & a_{2s} \\ \cdots & \cdots & \cdots & \cdots \\ a_{m1} & a_{m2} & \cdots & a_{ms} \end{pmatrix},\qquad B=\begin{pmatrix} b_{11} & b_{12} & \cdots & b_{1n} \\ b_{21} & b_{22} & \cdots & b_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ b_{s1} & b_{s2} & \cdots & b_{sn} \end{pmatrix}$$

且

$$ {}^tA = (a'_{ki}), \qquad {}^tB = (b'_{jk}), $$

那么

$$ a'_{ki} = a_{ik}, \qquad b'_{jk} = b_{kj}. $$

计算下述矩阵的元素

$$ C = AB = \begin{pmatrix} c_{11} & c_{12} & \cdots & c_{1n} \\ c_{21} & c_{22} & \cdots & c_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ c_{m1} & c_{m2} & \cdots & c_{mn} \end{pmatrix}, \qquad D = {}^tB{}^tA = \begin{pmatrix} d_{11} & d_{12} & \cdots & d_{1m} \\ d_{21} & d_{22} & \cdots & d_{2m} \\ \cdots & \cdots & \cdots & \cdots \\ d_{n1} & d_{n2} & \cdots & d_{nm} \end{pmatrix} $$

根据公式 (7):

$$ c_{ij} = \sum_{k=1}^{n} a_{ik}b_{kj}, \quad d_{ji} = \sum_{k=1}^{n} b'_{jk}a'_{ki} = \sum_{k=1}^{n} a_{ik}b_{kj}, $$

表明 $d_{ji} = c_{ij}$ 对一切 $1 \leqslant i \leqslant m, 1 \leqslant j \leqslant n$ 成立. 因而 ${}^tC = D$, 或用原来的记法,

$$ {}^t(AB) = B^tA^t. $$

更一般地，如果矩阵 $A_1, A_2, \cdots, A_r$ 的乘积有定义，则

$$ {}^t(A_1A_2\cdots A_r) = {}^tA_r \cdots {}^tA_2{}^tA_1. $$

由于 §2 定理 1, 性质 $\mathrm{rank}\,{}^tA = \mathrm{rank}A$ 成立.

4. 矩阵乘积的秩 设 A 和 B 是阶分别为 $m \times s$ 和 $s \times n$ 的任意两个矩阵. 关于 $\mathrm{rank}AB$ 可以知道些什么呢？

定理 3 *不等式*

$$ \mathrm{rank}AB \leqslant \min\{\mathrm{rank}A, \mathrm{rank}B\} $$

成立.

证明 公式 (7) 给出了矩阵 $C = AB$ 的行 $C_{(i)}$ 和列 $C^{(j)}$ 的表达式

$$ C_{(i)} = A_{(i)}B, \qquad C^{(j)} = AB^{(j)}. \tag{11} $$

矩阵 A 的秩可解释成

$$ r_1 = \mathrm{rank}A = \dim\langle A_{(1)}, A_{(2)}, \cdots, A_{(m)}\rangle, $$

不失一般性, 我们把 $A_{(1)}, \cdots, A_{(r_1)}$ 当作行向量基, 因为 A 当中行的变换, 附带引起了 C 当中行的变换. 但这种变换 (I 型初等变换) 既不改变 $\mathrm{rank}A$, 也不改变 $\mathrm{rank}C$. 于是

$$ A_{(k)} = \sum_{i=1}^{r_1} \lambda_{ki}A_{(i)}, \quad r_1 < k \leqslant m, $$

我们 (运用分配律 (10)) 得到

$$C_{(k)} = A_{(k)}B = \left(\sum_{i=1}^{r_1} \lambda_{ki} A_{(i)}\right) B = \sum_{i=1}^{r_1} \lambda_{ki}(A_{(i)}B) = \sum_{i=1}^{r_1} \lambda_{ki} C_{(i)},$$

于是

$$\langle C_{(1)}, \cdots, C_{(m)} \rangle = \langle C_{(1)}, \cdots, C_{(r_1)} \rangle.$$

这时

$$\text{rank}C = \dim\langle C_{(1)}, \cdots, C_{(m)} \rangle \leqslant r_1 = \text{rank}A.$$

类似地将矩阵 B 的秩看作

$$r_2 = \text{rank}B = \dim\langle B^{(1)}, B^{(2)}, \cdots, B^{(n)} \rangle,$$

并不失一般性将 $B^{(1)}, \cdots, B^{(r_2)}$ 作为列向量基，我们有

$$\begin{aligned} B^{(k)} &= \sum_{j=1}^{r_2} \mu_{kj} B^{(j)}, C^{(k)} = AB^{(k)} = A\left(\sum_{j=1}^{r_2} \mu_{kj} B^{(j)}\right) \\ &= \sum_{j=1}^{r_2} \mu_{kj} AB^{(j)} = \sum_{j=1}^{r_2} \mu_{kj} C^{(j)}, \\ & r_2 < k \leqslant n, \end{aligned}$$

从而

$$\text{rank}C = \dim\langle C^{(1)}, \cdots, C^{(n)} \rangle \leqslant r_2 = \text{rank}B. \qquad \square$$

我们指出，在某些情况下，定理 3 中的不等式可以是严格的. 例如当 $A \neq 0, B \neq 0$ 时，可能有 $AB = 0$(见第 2 段例 2). 一般来说，定理 3 只能简单地断定，矩阵乘积的秩不会增大.

5. 方阵 全体 n 阶实方阵 (a_{ij}) 的集合通常记作 $M_n(\mathbb{R})$(或 M_n). 我们在第 1 段结尾处已经指出，亦可称这一集合为向量空间 $M_n(\mathbb{R})$. 根据第 2 段， $M_n(\mathbb{R})$ 中任意两个矩阵的乘积仍在 $M_n(\mathbb{R})$ 中，且满足结合律和分配律.

定义 *称 n 阶方阵的集合构成一个* **(结合) 环**.

不难验证纯量乘法满足 $\lambda AB = (\lambda A)B = A(\lambda B)$, 其中 $\lambda \in \mathbb{R}$, 考虑到这一点，集合 $M_n(\mathbb{R})$ 也叫作一个 $\mathbb{R}$ 上的 **代数**.

我们要逐步习惯于使用这些名词 (关于术语化新对象的分类见第 4 章), 现在我们转到单位矩阵 $E = (\delta_{kj})$, 此处

$$\delta_{kj} = \begin{cases} 1 & 若\ k = j, \\ 0 & 若\ k \neq j, \end{cases}$$

叫作 **克罗内克符号**. 显然 $\mathrm{rank}E = n$. 用 δ_{kj} 代替 b_{kj}, 矩阵相乘的法则 (7) 给出了下述关系式:

$$EA = A = AE, \qquad A \in M_n(\mathbb{R}).$$

更一般地:

$$\mathrm{diag}_n(\lambda)A = \lambda A = A\mathrm{diag}_n(\lambda), \tag{12}$$

其中

$$\mathrm{diag}_n(\lambda) = \lambda E = \begin{vmatrix} \lambda & 0 & \cdots & 0 \\ 0 & \lambda & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & \lambda \end{vmatrix}$$

是我们已经知道的纯量矩阵 (见第 1 章 §3). 所以矩阵 A 与纯量 λ 的乘积等于 A 与纯量阵的乘积.

等式 (12) 给出了一个显而易见的事实, 纯量阵 $\mathrm{diag}_n(\lambda)$ 与任意矩阵 A 可交换. 它的逆命题在应用中十分重要.

定理 4 *在 M_n 中, 与任意矩阵可交换的矩阵是纯量阵.*

证明 引入矩阵 E_{ij}, 它在第 i 行第 j 列的交点处取值 1, 而所有其他的元素均为零. 如果 $Z = (z_{ij})$ 是定理中要求的矩阵, 则特别地, Z 与所有的 E_{ij} 可交换:

$$ZE_{ij} = E_{ij}Z, \quad i, j = 1, 2, \cdots, n.$$

在这一等式的左右两边做矩阵乘法, 我们得到矩阵

$$\begin{pmatrix} 0 & \cdots & z_{1i} & \cdots & 0 \\ 0 & \cdots & z_{2i} & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & \cdots & \underset{(j)}{z_{ni}} & \cdots & 0 \end{pmatrix} \text{和} \begin{pmatrix} 0 & 0 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ z_{j1} & z_{j2} & \cdots & z_{jn} \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 0 \end{pmatrix} (i)$$

它们分别有唯一非零的第 j 列和唯一非零的第 i 行. 比较两个矩阵, 立即得关系式 $z_{ki} = 0$ 若 $k \neq i$, 以及 $z_{ii} = z_{jj}$. 改变 i 和 j, 定理得证. □

对给定矩阵 $A \in M_n(\mathbb{R})$, 可以试着去找一个矩阵 $A' \in M_n(\mathbb{R})$, 满足关系式 $AA' = E = A'A$. 易见

$$AA' = E = A''A \Longrightarrow A'' = A'. \tag{13}$$

事实上, $A'' = A''E = A''(AA') = (A''A)A' = EA' = A'$. 这样, 若矩阵 A' 存在, 必定唯一. 它叫作矩阵 A 的 **逆矩阵**, 记作 A^{-1} :

$$AA^{-1} = E = A^{-1}A. \tag{14}$$

如果 (14) 式满足，称矩阵 A 是 **可逆的**.

定义 矩阵 $A \in M_n(\mathbb{R})$ 叫作 **非退化的**, 如果它的行 (同样地列) 向量组是线性无关的，即 $\mathrm{rank}A = n$. 如果 $\mathrm{rank}A < n$, 则 A 叫作 **退化的**.

定理 5 矩阵 $A \in M_n(\mathbb{R})$ 是可逆的，当且仅当 A 是非退化的.

证明 1) 如果 $AB = E$(或 $BA = E$), 则由定理 3 有

$$n = \mathrm{rank}E = \mathrm{rank}AB \leqslant \min\{\mathrm{rank}A, \mathrm{rank}B\} \leqslant n,$$

从而 $\mathrm{rank}A = n$.

2) 如果 $\mathrm{rank}A = n$, 则

$$\langle E^{(1)}, \cdots, E^{(n)} \rangle = \mathbb{R}^n = \langle A^{(1)}, \cdots, A^{(n)} \rangle,$$

于是

$$E^{(j)} = \sum_{i=1}^{n} a'_{ij} A^{(i)}, \qquad 1 \leqslant j \leqslant n, \tag{15}$$

并且元素 a'_{ij} 组成的矩阵 $A' = (a'_{ij}) \in M_n(\mathbb{R})$ 是唯一确定的. 根据 §2 第 1 段 (见那里的等式 (1) 和 (2)), 关系式 (15) 可以写成

$$E^{(j)} = AA'^{(j)}, \qquad 1 \leqslant j \leqslant n,$$

所以

$$E = (E^{(1)}, \cdots, E^{(n)}) = (AA'^{(1)}, \cdots, AA'^{(n)}) = AA'.$$

此处我们将矩阵 E 和 AA' 都用它们的列来表示.

我们指出 (见第 3 段)A 的转置矩阵 ${}^tA$ 也与 A 一样是非退化的. 因而可以找到矩阵 B, 使 ${}^tA \cdot B = E$. 回到第 3 段并令 $A'' = {}^tB$, 我们有

$$E = {}^tE = {}^t({}^tAB) = {}^tB\,{}^t({}^tA) = A''A.$$

于是

$$AA' = E = A''A.$$

根据 (13) 式， $A'' = A'$, 所以按照 (14) 式， $A' = A^{-1}$, 即矩阵 A 是可逆的. □

推论 1 如果 B 和 C 分别是 m 阶和 n 阶的非退化方阵，而 A 是任意的 $m \times n$ 矩阵，则

$$\mathrm{rank}BAC = \mathrm{rank}A.$$

证明 由于定理 3 和 5, 我们有

$$\begin{aligned}\mathrm{rank}BAC &\leqslant \mathrm{rank}BA = \mathrm{rank}BA(CC^{-1}) \\ &= \mathrm{rank}(BAC)C^{-1} \leqslant \mathrm{rank}BAC,\end{aligned}$$

得到 $\mathrm{rank}BAC = \mathrm{rank}BA$. 类似地可建立等式

$$\mathrm{rank}BA = \mathrm{rank}A. \qquad \square$$

推论 2 如果 $A, B \in M_n(\mathbb{R})$ 且 $AB = E$ 或 $BA = E$, 则 $B = A^{-1}$.

证明 见定理 5 证明的第 1) 部分, $AB = E \Rightarrow \mathrm{rank}A = n$, 即 A 是非退化的, 从而是可逆的. $\square$

推论 3 如果 $A, B, \cdots, C, D$ 是非退化的 $n \times n$ 矩阵, 则乘积 $AB \cdots CD$ 也是非退化的, 且

$$(AB \cdots CD)^{-1} = D^{-1}C^{-1} \cdots B^{-1}A^{-1}.$$

证明 矩阵 $G = AB \cdots CD$ 的非退化性由推论 1 给出, 而等式 $G^{-1} = D^{-1}C^{-1} \cdots B^{-1}A^{-1}$ 可直接验证:

$$\begin{aligned} G(D^{-1}C^{-1} \cdots B^{-1}A^{-1}) &= AB \cdots C(DD^{-1})C^{-1} \cdots B^{-1}A^{-1} \\ &= AB \cdots (CC^{-1}) \cdots B^{-1}A^{-1} = \cdots = E. \end{aligned} \qquad \square$$

实际计算逆矩阵的常用方法将在第 7 段给出. 在那里也同时得到了定理 5 的另一种证明.

我们将在第 3 章给出 A^{-1} 的一个显式. 现在仅仅指出, 给定实系数矩阵 A, 实际计算 A^{-1}, 或者计算两个矩阵的乘积, 需要完成大量的运算. 在应用中会遇到阶数 $n = 100$ 或更大的矩阵. 如果 A 和 B 是这样的两个矩阵, 计算 $C = AB$ 需要按照公式 (7)(或 (9)) 找到 n^2 个元素 c_{ij}, 每找一个元素要做 $(2n-1)$ 次乘法或加法. 共需进行 $(2n-1)n^2$ 次运算, 也就是说当 $n = 100$ 时要做约二百万次运算. 对于现代的计算机, 这个问题不难, 但如果我们想找到矩阵 A 的方幂 A^m, 且 $m \geqslant 1\,000$, 计算机实现就会发生困难. 根据定义, $A^m = A \cdot A^{m-1}$; 但由结合律 (见定理 2 的推论) 易见 $A^m = A^k A^{m-k}, 0 \leqslant k \leqslant m$, 这将在第四章中在更一般的背景下进行说明. 为了计算 A^m, 人们使用各种附加的手段, 它们或者基于矩阵 A 的特殊性质, 或者借用于线性代数课程作为解释. 我们来看三个例子.

例 1 如果

$$A = \mathrm{diag}(\alpha_1, \cdots, \alpha_n) = \begin{pmatrix} \alpha_1 & \cdots & 0 \\ \cdots & \cdots & \cdots \\ 0 & \cdots & \alpha_n \end{pmatrix},$$

则显然

$$A^m = \mathrm{diag}(\alpha_1^m, \cdots, \alpha_n^m) = \begin{pmatrix} \alpha_1^m & \cdots & 0 \\ \cdots & \cdots & \cdots \\ 0 & \cdots & \alpha_n^m \end{pmatrix}.$$

例 2 设

$$A=\begin{pmatrix} a & c \\ 0 & b \end{pmatrix}.$$

对 m 作归纳表明,

$$A^m=\begin{pmatrix} a^m & c\dfrac{a^m-b^m}{a-b} \\ 0 & b^m \end{pmatrix},$$

此处

$$\frac{a^m-b^m}{a-b}=a^{m-1}+a^{m-2}b+\cdots+ab^{m-2}+b^{m-1}.$$

特别地, 若 $a=b$, 有

$$\begin{pmatrix} a & c \\ 0 & a \end{pmatrix}^m=\begin{pmatrix} a^m & ma^{m-1}c \\ 0 & a^m \end{pmatrix}.$$

例 3 对 m 用归纳法, 不难证明矩阵

$$A=\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$$

的 m 次方幂形如

$$A^m=\begin{pmatrix} f_{m-1} & f_m \\ f_m & f_{m+1} \end{pmatrix}, \tag{16}$$

其中整数 $f_0=0, f_1=1, f_2=1, f_3=2, \cdots$, 它们是用递归关系式

$$f_{m+1}=f_m+f_{m-1}$$

定义的. 这些正是斐波那契数 (见第 1 章 §3 末的例 2).

引进行列式为 1 的矩阵 (见第 1 章 §4)

$$B=\begin{pmatrix} -\dfrac{\lambda_2}{5} & \dfrac{1}{5} \\ -\sqrt{5}\lambda_1 & \sqrt{5} \end{pmatrix},$$

其中 $\lambda_1=\dfrac{1+\sqrt{5}}{2},\lambda_2=\dfrac{1-\sqrt{5}}{2}$.

不难计算,

$$B^{-1}=\begin{pmatrix}\sqrt{5} & -\dfrac{1}{5}\\ \sqrt{5}\lambda_1 & -\dfrac{\lambda_2}{5}\end{pmatrix},\quad A=B^{-1}\cdot\begin{pmatrix}\lambda_1 & 0\\ 0 & \lambda_2\end{pmatrix}\cdot B.$$

但是如果三个 $n\times n$ 矩阵 A,B,C, 其中 B 是非退化的, 满足关系式 $A=B^{-1}CB$, 则

$$A^m=B^{-1}CB\cdot B^{-1}CB\cdot B^{-1}CB\cdots B^{-1}CB=B^{-1}C^mB$$

(其中的因子 BB^{-1} 等于 E, 约去). 在这种情况下, 考虑到例 1 和关系式 (16) 有

$$\begin{aligned}\begin{pmatrix}f_{m-1} & f_m\\ f_m & f_{m+1}\end{pmatrix}&=A^m=B^{-1}\begin{pmatrix}\lambda_1 & 0\\ 0 & \lambda_2\end{pmatrix}^m B=B^{-1}\begin{pmatrix}\lambda_1^m & 0\\ 0 & \lambda_2^m\end{pmatrix}B\\
&=\begin{pmatrix}\sqrt{5} & -\dfrac{1}{5}\\ \sqrt{5}\lambda_1 & -\dfrac{\lambda_2}{5}\end{pmatrix}\begin{pmatrix}\lambda_1^m & 0\\ 0 & \lambda_2^m\end{pmatrix}B\\
&=\begin{pmatrix}\sqrt{5}\lambda_1^m & -\dfrac{1}{5}\lambda_2^m\\ \sqrt{5}\lambda_1^{m+1} & -\dfrac{1}{5}\lambda_2^{m+1}\end{pmatrix}\begin{pmatrix}-\dfrac{\lambda_2}{5} & \dfrac{1}{5}\\ -\sqrt{5}\lambda_1 & \sqrt{5}\end{pmatrix}\\
&=\begin{pmatrix}* & \dfrac{1}{\sqrt{5}}(\lambda_1^m-\lambda_2^m)\\ * & *\end{pmatrix}\end{aligned}$$

($*$ 代表我们不感兴趣的数).

比较这些等式中第一个和最后一个右上角的元素, 得到第 m 个斐波那契数的公式

$$f_m=\frac{\lambda_1^m-\lambda_2^m}{\sqrt{5}}=\frac{1}{\sqrt{5}}\left\{\left(\frac{1+\sqrt{5}}{2}\right)^m-\left(\frac{1-\sqrt{5}}{2}\right)^m\right\}.$$

因为 $\lim\limits_{m\to\infty}\left(\dfrac{1-\sqrt{5}}{2}\right)^m=0$, 我们看到当 m 充分大时, $f_m\sim\dfrac{1}{\sqrt{5}}\lambda_1^m$ (近似于几何级数).

6. 矩阵的等价类 如同定理 4 的证明中所述, 我们用 E_{st} 记 $m\times m$ 矩阵, 其中第 s 行与第 t 列交叉处的元素为 1, 所有其他的元素为 0(这样的矩阵叫作 **矩阵单位**). 研究 $M_m(\mathbb{R})$ 中下述形式的 **初等矩阵**:

$$F_{s,t}=E-E_{s,s}-E_{t,t}+E_{s,t}+E_{t,s}$$

$$
= \begin{pmatrix} 1 & & & & & & \\ & \ddots & & & & & \\ & & 0 & & 1 & & \\ & & & \ddots & & & \\ & & & 1 & & & \\ & & & & \ddots & & \\ & & 1 & & 0 & & \\ & & & & & \ddots & \\ & & & & & & 1 \end{pmatrix}, \quad s \neq t; \qquad (\mathrm{I})
$$

$$
F_{s,t}(\lambda) = E + \lambda E_{s,t} = \begin{pmatrix} 1 & & & & & & \\ & \ddots & & & & & \\ & \cdots & 1 & \cdots & \lambda & \cdots & \\ & & & \ddots & & & \\ & & & & \ddots & & \\ & & & & & & 1 \end{pmatrix}, \quad s \neq t; \qquad (\mathrm{II})
$$

$$
F_s(\lambda) = E + (\lambda - 1)E_{s,s} = \mathrm{diag}\{1, \cdots, 1, \lambda, 1, \cdots, 1\}, \quad \lambda \neq 0. \qquad (\mathrm{III})
$$

设 A 是任意的 $m \times n$ 矩阵. 直接验证可知, 如果 $F = F_{s,t}$ 或 $F = F_{s,t}(\lambda)$, 矩阵 $A' = FA$ 是从 A 通过施行对行的 (I) 型或 (II) 型初等变换得到的.

如果 $F = F_s(\lambda)$, 我们有 (III) 型初等变换 (用 λ 乘以 A 的第 s 行 $A_{(s)}$). 类似地, 矩阵 $A'' = AF$ 可以从 A 施行初等列变换得到. 我们从 §2 第 2 段和 §2 习题 2 知道, 对行和列施行 (I) 型和 (II) 型初等变换, A 可以化成一个左上角为 $r \times r$ 非退化对角子阵的矩阵, 此处 $r = \mathrm{rank} A$(当 $r = 0$ 时, A 是零矩阵). 因为

$$
\begin{pmatrix} a_1 & & & & & & \\ & a_2 & & & 0 & & \\ & & \ddots & & & & \\ & & & a_r & & & \\ & 0 & & & 0 & & \\ & & & & & \ddots & \\ & & & & & & 0 \end{pmatrix}
$$

$$= F_1(a_1)F_2(a_2)\cdots F_r(a_r)\begin{pmatrix} 1 & & & & & & \\ & 1 & & & & 0 & \\ & & \ddots & & & & \\ & & & 1 & & & \\ & & & & 0 & & \\ & & 0 & & & \ddots & \\ & & & & & & 0 \end{pmatrix},$$

允许施行 (Ⅲ) 型初等变换，便可以从 A 得到下述形状的矩阵

$$\begin{pmatrix} E_r & 0 \\ 0 & 0 \end{pmatrix} \tag{17}$$

(这里 E_r 是 $M_r(\mathbb{R})$ 中的单位矩阵；三个零分别表示阶为 $r\times(n-r),(m-r)\times r$ 以及 $(m-r)\times(m-r)$ 的零矩阵). 这样

$$P_kP_{k-1}\cdots P_1AQ_1Q_2\cdots Q_l = \begin{pmatrix} E_r & 0 \\ 0 & 0 \end{pmatrix}, \tag{18}$$

其中 $P_i(Q_i)$ 是 m 阶 (相应地 n 阶) 初等矩阵.

多次提及初等变换是可逆的. 这与初等矩阵的可逆性是一致的：

$$(F_{s,t})^{-1} = F_{s,t},\quad F_{s,t}(\lambda)^{-1} = F_{s,t}(-\lambda),\quad F_s(\lambda)^{-1} = F_s(\lambda^{-1}).$$

根据定理 5 的推论 3, 矩阵 $P = P_kP_{k-1}\cdots P_1$ 和 $Q = Q_1Q_2\cdots Q_l$ 也可逆：

$$P^{-1} = P_1^{-1}\cdots P_{k-1}^{-1}P_k^{-1},\quad Q^{-1} = Q_l^{-1}\cdots Q_2^{-1}Q_1^{-1}.$$

注意 P_i^{-1}, Q_j^{-1} 都是初等矩阵.

称两个 $m\times n$ 阶矩阵 A, B 是**等价的**, 并记作 $A\sim B$, 如果能够找到非退化的 m 阶和 n 阶矩阵 P, Q, 使得 $B = PAQ$.

易见 $\sim$ 是一个等价关系：

i) $A\sim A(P = E_m, Q = E_n)$;

ii) $A\sim B \Rightarrow B\sim A$, 因为 $B = PAQ \Rightarrow A = P^{-1}BQ^{-1}$;

iii) $B = P'AQ', C = P''BQ'' \Rightarrow C = PAQ$, 其中 $P = P''P', Q = Q'Q''$.

根据一般原则 (见第 1 章 §6), 所有的 $m\times n$ 矩阵的集合按照关系 $\sim$ 划分成互不相交的等价矩阵类. 因为等价矩阵的秩相等 (见定理 5 的推论 1), 等式 (18) 的论证表明，可以选择矩阵 (17) 作为等价类的代表元.

我们得到了下述论断.

定理 6 $m\times n$ 矩阵的集合划分成 $p=\min\{m,n\}+1$ 个等价类. 所有秩为 r 的矩阵都和代表元 (17) 在同一类中.

推论 每一个非退化的 $n\times n$ 矩阵都可以写成初等矩阵的乘积.

证明 所有非退化的 n 阶矩阵都和单位矩阵在同一个等价类中, 因为它们的秩等于 n. 将关系式 (18)

$$P_kP_{k-1}\cdots P_1AQ_1Q_2\cdots Q_l=E,$$

改写成

$$A=P_1^{-1}\cdots P_{k-1}^{-1}P_k^{-1}Q_l^{-1}\cdots Q_2^{-1}Q_1^{-1},\tag{19}$$

推论得证. □

不能断定将 A 写成初等矩阵的乘积时写法是唯一的, 但这种写法的存在性本身就已经非常有用. 特别地, 它可以用来求逆矩阵. 事实上, 从公式 (19) 我们得到

$$A^{-1}=Q_1Q_2\cdots Q_lP_kP_{k-1}\cdots P_1=QP.$$

7. 逆矩阵的计算 在上一段的推论中, 如果只做行变换, 当 $A\in M_n(\mathbb{R})$ 非退化时, 从 $n\times 2n$ 阶的扩展矩阵 $(A|E)$ 开始, 就会得到一系列变换

$$(A|E)\xrightarrow{P_1}(P_1A|P_1E)\xrightarrow{P_2}\cdots\xrightarrow{P_k}(P_k\cdots P_2P_1A|P_k\cdots P_2P_1E)=(E|A').$$

这个序列在第 k 步中止, 直到 $n\times 2n$ 阶矩阵左半边的 A 换成了单位矩阵 E. 这时右半边得到了唯一的矩阵: $A'=A^{-1}$. 如果矩阵 A 退化, 这个过程可能中断得早些, 我们将 A 化成了阶梯形并得到了秩 $r=\operatorname{rank}A$.

在第 6 节开头, 取 $n=3$, 我们有初等矩阵的实例

$$F_{1,2}(-3)=\begin{pmatrix}1&-3&0\\0&1&0\\0&0&1\end{pmatrix},F_{3,2}(4)=\begin{pmatrix}1&0&0\\0&1&0\\0&4&1\end{pmatrix},F_{1,3}=\begin{pmatrix}0&0&1\\0&1&0\\1&0&0\end{pmatrix}.$$

左乘 $n\times n$ 初等矩阵 P_i 的作用未加阐述. 事实上, 它可以看作一个指令, 完成与之相应的初等行变换.

再次提醒读者注意下述符号的含义:

$P_i=F_{s,t}$—— 将矩阵的第 s 和 t 行交换位置;

$P_i=F_{s,t}(\lambda)$—— 将矩阵的第 t 行乘以 λ 加到第 s 行上;

$P_i=F_s(\lambda)$—— 将矩阵的第 s 行乘以 λ.

例 4 设

$$A=\begin{pmatrix}0&2&0\\1&1&-1\\2&1&-1\end{pmatrix}$$

我们有

$$(A|E)=\left(\begin{array}{ccc|ccc}0&2&0&1&0&0\\1&1&-1&0&1&0\\2&1&-1&0&0&1\end{array}\right)\xrightarrow{F_{1,2}}\left(\begin{array}{ccc|ccc}1&1&-1&0&1&0\\0&2&0&1&0&0\\2&1&-1&0&0&1\end{array}\right)\xrightarrow{F_{3,1}(-2)}$$

$$\left(\begin{array}{ccc|ccc}1&1&-1&0&1&0\\0&2&0&1&0&0\\0&-1&1&0&-2&1\end{array}\right)\xrightarrow{F_2(\frac{1}{2})}\left(\begin{array}{ccc|ccc}1&1&-1&0&1&0\\0&1&0&\frac{1}{2}&0&0\\0&-1&0&0&-2&1\end{array}\right)\xrightarrow{F_{1,2}(-1)}$$

$$\left(\begin{array}{ccc|ccc}1&0&-1&-\frac{1}{2}&1&0\\0&1&0&\frac{1}{2}&0&0\\0&-1&1&0&-2&1\end{array}\right)\xrightarrow{F_{3,2}(1)}\left(\begin{array}{ccc|ccc}1&0&-1&-\frac{1}{2}&1&0\\0&1&0&\frac{1}{2}&0&0\\0&0&1&\frac{1}{2}&-2&1\end{array}\right)\xrightarrow{F_{1,3}(1)}$$

$$\left(\begin{array}{ccc|ccc}1&0&0&0&-1&1\\0&1&0&\frac{1}{2}&0&0\\0&0&1&\frac{1}{2}&-2&1\end{array}\right).$$

所以

$$A^{-1}=\begin{pmatrix}0&-1&1\\\frac{1}{2}&0&0\\\frac{1}{2}&-2&1\end{pmatrix}.$$

为了书写简便，我们可以适当地将同类型的变换同时进行.

例 5 设

$$A=\begin{pmatrix}-1&1&1&1\\1&-1&1&1\\1&1&-1&1\\1&1&1&-1\end{pmatrix}.$$

我们有

$$(A|E)=\left(\begin{array}{cccc|cccc}-1&1&1&1&1&0&0&0\\1&-1&1&1&0&1&0&0\\1&1&-1&1&0&0&1&0\\1&1&1&-1&0&0&0&1\end{array}\right)$$

$$\xrightarrow[F_{1,2}(1)]{F_{1,4}(1) \atop F_{1,3}(1)} \left(\begin{array}{cccc|cccc} 2 & 2 & 2 & 2 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & -1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & -1 & 0 & 0 & 0 & 1 \end{array}\right)$$

$$\xrightarrow{F_1(\frac{1}{2})} \left(\begin{array}{cccc|cccc} 1 & 1 & 1 & 1 & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} \\ 1 & -1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & -1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & -1 & 0 & 0 & 0 & 1 \end{array}\right)$$

$$\xrightarrow[F_{2,1}(-1)]{F_{4,1}(-1) \atop F_{3,1}(-1)} \left(\begin{array}{cccc|cccc} 1 & 1 & 1 & 1 & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} \\ 0 & -2 & 0 & 0 & -\frac{1}{2} & \frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} \\ 0 & 0 & -2 & 0 & -\frac{1}{2} & -\frac{1}{2} & \frac{1}{2} & -\frac{1}{2} \\ 0 & 0 & 0 & -2 & -\frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} & \frac{1}{2} \end{array}\right)$$

$$\xrightarrow[F_2(-\frac{1}{2})]{F_4(-\frac{1}{2}) \atop F_3(-\frac{1}{2})} \left(\begin{array}{cccc|cccc} 1 & 1 & 1 & 1 & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} \\ 0 & 1 & 0 & 0 & \frac{1}{4} & -\frac{1}{4} & \frac{1}{4} & \frac{1}{4} \\ 0 & 0 & 1 & 0 & \frac{1}{4} & \frac{1}{4} & -\frac{1}{4} & \frac{1}{4} \\ 0 & 0 & 0 & 1 & \frac{1}{4} & \frac{1}{4} & \frac{1}{4} & -\frac{1}{4} \end{array}\right)$$

$$\xrightarrow[F_{1,2}(-1)]{F_{1,4}(-1) \atop F_{1,3}(-1)} \left(\begin{array}{cccc|cccc} 1 & 0 & 0 & 0 & -\frac{1}{4} & \frac{1}{4} & \frac{1}{4} & \frac{1}{4} \\ 0 & 1 & 0 & 0 & \frac{1}{4} & -\frac{1}{4} & \frac{1}{4} & \frac{1}{4} \\ 0 & 0 & 1 & 0 & \frac{1}{4} & \frac{1}{4} & -\frac{1}{4} & \frac{1}{4} \\ 0 & 0 & 0 & 1 & \frac{1}{4} & \frac{1}{4} & \frac{1}{4} & -\frac{1}{4} \end{array}\right).$$

所以, $A^{-1} = \dfrac{1}{4}A$.

在上例中, 计算亦可避免. 注意到退化矩阵与任意矩阵的乘积都是退化的 (定理 3), 但我们有

$$A^2 = \begin{pmatrix} 4 & 0 & 0 & 0 \\ 0 & 4 & 0 & 0 \\ 0 & 0 & 4 & 0 \\ 0 & 0 & 0 & 4 \end{pmatrix} = 4E;$$

因而 A 非退化, A^{-1} 是存在的.

$$A = A^2A^{-1} = 4E \cdot A^{-1} = 4A^{-1} \Longrightarrow A^{-1} = \frac{1}{4}A.$$

注记 在施行系列初等行变换时, 应当避免一个典型的错误 —— 将前一个变换中改变了的行加到未改变的行上. 例如算法

$$A \underset{F_{1,2}(1)}{\overset{F_{2,1}(1)}{\longrightarrow}} A'$$

是模棱两可的: 不清楚其中作用的顺序, 先 $F_{1,2}(1)$, 后 $F_{2,1}(1)$; 先 $F_{2,1}(1)$, 后 $F_{1,2}(1)$, 或同时进行? 不同的方式得到了行 $A'_{(1)}, A'_{(2)}$ 的不同表达. 在例 5 中, 我们合并的只是同类型的变换, 而如果我们打算按照上述方法用计算机进行计算, 那么线性调整初等变换的序列是自然的.

上述求矩阵的秩以及逆矩阵的方法, 叫作 ***P*约化**, 或更一般地, 矩阵到 *标准型*(17) 的 **(P, Q)约化**.

8. 解空间 从 §2 和 §3 开头的导言得知, 带有 $m \times n$ 阶系数矩阵 A 和自由项 $B \in \mathbb{R}^m$ 的线性方程组可以写成

$$AX = B \tag{20}$$

(其中 $X = [x_1, \cdots, x_n]$ 是高度为 n 的列). 假设 $m = n$ 且方阵 A 非退化 (见第 5 段), 用 A^{-1} 左乘矩阵等式的两端: $X = EX = (A^{-1}A)X = A^{-1}(AX) = A^{-1}B$, 我们得到方程组 (20) 的解, 并且该解是唯一的. 解的这种方便的写法并没有使我们免去必要的计算, 因为 A^{-1} 并未预先给定. 但我们仍然满意地指出, 矩阵工具的运用至少使人得到了美学上的快感. 现在我们运用这一工具来求齐次线性方程组

$$AX = 0 \tag{21}$$

的全部解. 先来看一个基本事实, 若 $X^{(1)}, X^{(2)}$ 是齐次线性方程组 (21) 的解, 则它们的任意线性组合也是 (21) 的解:

$$A(\alpha_1 X^{(1)} + \alpha_2 X^{(2)}) = \alpha_1 AX^{(1)} + \alpha_2 AX^{(2)} = 0.$$

因而可以谈论齐次线性方程组的 *解空间*—— 线性包:

$$V_A = \langle X \in \mathbb{R}^n | AX = 0 \rangle \subset \mathbb{R}^n.$$

设 $s = \dim V_A, r = \operatorname{rank} A$. 根据定义 $s \leqslant n, r \leqslant \min\{m, n\}$. 那么 s 与 r 之间存在什么联系呢?

定理 7 *等式 $r + s = n$ 成立.*

证明 选择线性包 V_A 的一组基 $X^{(1)},\cdots,X^{(s)}$，并扩充成全空间 $\mathbb{R}^n$ 的基 $X^{(1)},\cdots,X^{(s)},X^{(s+1)},\cdots,X^{(n)}$. 如同 §1 定理 2 的证明 (或 §1 习题 6) 所指出的，这件事总能办到，任取向量 $X=\sum\limits_{i=1}^{n}\alpha_iX^{(i)}\in\mathbb{R}^n$, 有

$$AX=\sum_{i=1}^{n}\alpha_iAX^{(i)}=\alpha_{s+1}AX^{(s+1)}+\cdots+\alpha_nAX^{(n)},$$

所以 §2 定义的线性包，称之为矩阵 A 的列空间，

$$\begin{aligned}V_{\rm c}(A)&=\langle A^{(1)},\cdots,A^{(n)}\rangle=\langle x_1A^{(1)}+\cdots+x_nA^{(n)}|x_i\in\mathbb{R}^n\rangle\\&=\langle AX|X\in\mathbb{R}^n\rangle\subset\mathbb{R}^m,\end{aligned}$$

与线性包 $\langle AX^{(s+1)},\cdots,AX^{(n)}\rangle$ 重合.

特别地，$r=\dim V_{\rm c}(A)\leqslant n-s$. 但是向量 $AX^{(s+1)},\cdots,AX^{(n)}$ 是线性无关的，因为从

$$0=\sum_{k\geqslant s+1}\beta_kAX^{(k)}=A(\sum_{k\geqslant s+1}\beta_kX^{(k)})$$

得到 $\sum\limits_{k\geqslant s+1}\beta_kX^{(k)}\in V_A$, 而由于 $X^{(s+1)},\cdots,X^{(n)}$ 的选择，仅有的可能性为 $\beta_{s+1}=\cdots=\beta_n=0$. 于是 $r=n-s$. □

注记 如果使用线性变换的语言 (见 §3 第 1 段), 显然有

$$V_A=\ker\varphi_A,\quad V_{\rm c}(A)=\operatorname{Im}\varphi_A,$$

即由 A 确定的线性变换 $\varphi_A:\mathbb{R}^n\to\mathbb{R}^m$ 的核与像. 对于我们来说，这种方法只是作为引入矩阵概念的一个说明.

为了找到空间 $V_{\rm c}(A)$ 的一组基, 我们要在 A 中选择 r 个列向量基, 方法之一是将 A 化为阶梯形，或者用第 3 章指出的办法置换矩阵的列，或等价地，重排未知量，可以使前 r 列 $A^{(1)},\cdots,A^{(r)}$ 成为列向量基. 这时，在关于未知量 $x'_1,x'_2,\cdots,x'_n$ 的新方程组中，$x'_1,\cdots,x'_r$ 成为主未知量. 任意 $r+1$ 个列向量 $A^{(1)},\cdots,A^{(r)},A^{(r+k)},k>0$, 都是线性相关的，根据 §1 的定理 1 v), 可以写出关系式

$$x_1^{(k)}A^{(1)}+x_2^{(k)}A^{(2)}+\cdots+x_r^{(k)}A^{(r)}+A^{(r+k)}=0,k=1,2,\cdots,n-r.$$

$(n-r)$ 个列向量

$$\begin{aligned}X^{(1)}&=\left[x_1^{(1)},x_2^{(1)},\cdots,x_r^{(1)},1,0,\cdots,0\right],\\X^{(2)}&=\left[x_1^{(2)},x_2^{(2)},\cdots,x_r^{(2)},0,1,\cdots,0\right],\\&\cdots\cdots\cdots\cdots\\X^{(n-r)}&=\left[x_1^{(n-r)},x_2^{(n-r)},\cdots,x_r^{(n-r)},0,0,\cdots,1\right]\end{aligned}\tag{22}$$

显然是线性无关的 (根据后 $n-r$ 个分量的特殊形式), 它们是齐次线性方程组 (21) 的解, 根据定理 7, 构成解空间 V_A 的一组基. 显然, 若 (带撇的) 新自由未知量取值

$$x'_{r+1}=0,\quad \cdots,\quad x'_{r+k}=1,\quad \cdots,\quad x'_n=0,$$

则得到解 $X^{(k)}$.

r 秩齐次线性方程组 $AX=0$ 的解空间的任意一组基称为一个 **基础解系**. 向量组 (22) 也叫作 **规范** 基础解系. 根据 §2 定理 1 的推论, 它的秩 $s=\dim V_A=n-r$, 等于该方程组的自由未知量的个数.

习　题

1. 在下述映射中, 哪些是线性映射:

a) $[x_1,x_2,\cdots,x_n]\mapsto[x_n,\cdots,x_2,x_1]$;

b) $[x_1,x_2,\cdots,x_n]\mapsto[x_1,x_2^2,\cdots,x_n^n]$;

c) $[x_1,x_2,\cdots,x_n]\mapsto[x_1,x_1+x_2,\cdots,x_1+x_2+\cdots+x_n]$.

2. 证明

$$\begin{pmatrix}1&a&c\\0&1&b\\0&0&1\end{pmatrix}^m=\begin{pmatrix}1&ma&\frac{m(m-1)}{2}ab+mc\\0&1&mb\\0&0&1\end{pmatrix}.$$

求矩阵

$$\begin{pmatrix}1&a&c\\0&1&b\\0&0&1\end{pmatrix}$$

的逆矩阵.

3. 验证 $\begin{pmatrix}0&-1\\1&-1\end{pmatrix}^3=E$.

4. 马尔可夫 (或随机) 矩阵在应用中十分重要:

$$P=(p_{ij}),\quad p_{ij}\geqslant 0,\quad \sum_{j=1}^{n}p_{ij}=1,\quad i=1,2,\cdots,n.$$

由马尔可夫矩阵确定的线性变换 φ_P 通常作用于概率列向量:

$$X=[x_1,\cdots,x_n],\quad x_i\geqslant 0,\quad \sum_{i=1}^{n}x_i=1.$$

从下述论断可见, 这些来自于自然科学问题的定义是协调的论断, 即便对 $n=2$, 也需要证明.

a) 矩阵 $P\in M_n(\mathbb{R})$ 是马尔可夫的, 当且仅当对任意概率向量 X, PX 仍然是概率向量 (此处 $PX=\varphi_P(X)$).

b) 如果 P 是正的马尔可夫矩阵(即 $\forall i,j,\quad p_{ij}>0$), 那么任意概率向量 X 对应到正的概率向量 PX(所有的分量严格大于 0).

c) 如果 P 和 Q 都是马尔可夫矩阵, 那么矩阵 PQ 也是马尔可夫矩阵. 特别地, 马尔可夫矩阵的任意次方幂 P^k 是马尔可夫矩阵.

5. 若

$$H=\begin{pmatrix}1&1&1&1\\1&-1&1&-1\\1&1&-1&-1\\1&-1&-1&1\end{pmatrix},$$

求 ${}^tH\cdot H$.

6. 由 S_n 中的 n 阶循环 (见第 1 章 §8) 确定的置换矩阵 (行单位阵 E_n) 为

$$P=\begin{pmatrix}0&0&\cdots&0&1\\1&0&\cdots&0&0\\0&1&\cdots&0&0\\ \cdots&\cdots&\cdots&\cdots&\cdots\\0&0&\cdots&0&0\\0&0&\cdots&1&0\end{pmatrix},$$

验证 $P^n=E$.

7. 对于任意两个 $m\times n$ 矩阵 A 和 B, 证明

$$\operatorname{rank}(A+B)\leqslant\operatorname{rank}A+\operatorname{rank}B.$$

8. 对于任意的 $m\times s$ 矩阵 A 和 $s\times n$ 矩阵 B, 证明

$$\operatorname{rank}A+\operatorname{rank}B-s\leqslant\operatorname{rank}AB.$$

9. 设 A,B,C 是 n 阶方阵, 若 $ABC=0$, 则

$$\operatorname{rank}A+\operatorname{rank}B+\operatorname{rank}C\leqslant 2n.$$

10. 求矩阵

$$A=\begin{pmatrix}x_1y_1&x_1y_2&\cdots&x_1y_n\\x_2y_1&x_2y_2&\cdots&x_2y_n\\ \cdots&\cdots&\cdots&\cdots\\x_ny_1&x_ny_2&\cdots&x_ny_n\end{pmatrix}$$

的秩.

提示: $A=[x_1,\cdots,x_n](y_1,\cdots,y_n)$.

11. 若 $A=(a_{ij})$ 是非退化对称矩阵 (即 $a_{ij}=a_{ji}$), 证明 A^{-1} 也是对称矩阵.

12. 设

$$A=\begin{pmatrix}5&4&3&2&1\\4&8&6&4&2\\3&6&9&6&3\\2&4&6&8&4\\1&2&3&4&5\end{pmatrix},\qquad F=\begin{pmatrix}2&3&2&1\\3&6&4&2\\4&8&6&3\\2&4&3&2\end{pmatrix},$$

求 A^{-1} 和 F^{-1}.

13. 验证

$$A=\begin{pmatrix}a&b\\c&d\end{pmatrix}, ad-bc\neq 0\Rightarrow A^{-1}=\frac{1}{ad-bc}\begin{pmatrix}d&-b\\-c&a\end{pmatrix}.$$

特别地,

$$ad-bc=1\Rightarrow A^{-1}=\begin{pmatrix}d&-b\\-c&a\end{pmatrix}.$$

如果 $ad-bc=0$, A^{-1} 存在吗?

14. 证明任意矩阵

$$A=\begin{pmatrix}a&b\\c&d\end{pmatrix}$$

满足关系式

$$A^2=(a+d)A-(ad-bc)E \tag{23}$$

(换言之, A 是二次方程 $x^2-(a+d)x+(ad-bc)=0$ 的一个 "根").

15. 如果 $ad-bc\neq 0$, 运用关系 (23) 求逆矩阵 A^{-1}.

16. 证明若 $\begin{pmatrix}a&b\\c&d\end{pmatrix}^m=0$, 则 $\begin{pmatrix}a&b\\c&d\end{pmatrix}^2=0$.

17. 阐明下述论断: 设 $m\times s$ 矩阵 X 被水平线和竖直线划分为块 (或长方块),

$$X=\begin{pmatrix}X_{11}&X_{12}&\cdots&X_{1k}\\X_{21}&X_{22}&\cdots&X_{2k}\\\cdots&\cdots&\cdots&\cdots\\X_{l1}&X_{l2}&\cdots&X_{lk}\end{pmatrix}$$

这里 $X_{i1},\cdots,X_{ik}$ 都是 m_i 行矩阵 $(m_1+\cdots+m_i=m)$, 而 $X_{1j},\cdots,X_{lj}$ 都是 s_j 列矩阵 $(s_1+\cdots+s_k=s)$.

如果

$$Y=\begin{pmatrix}Y_{11}&Y_{12}&\cdots&Y_{1r}\\Y_{21}&Y_{22}&\cdots&Y_{2r}\\\cdots&\cdots&\cdots&\cdots\\Y_{k1}&Y_{k2}&\cdots&Y_{kr}\end{pmatrix}$$

是一个 $s\times n$ 矩阵, 它的块 Y_{ij} 的阶是 $s_i\times n_j(n_1+\cdots+n_r=n)$, 则乘积 $Z=XY$ 是有意义的, 并且矩阵 $Z=(z_{ij})$ 可以分块计算, 它的块 Z_{ij} 可按公式 (7) 形式地写出:

$$Z_{ij}=X_{i1}Y_{1j}+X_{i2}Y_{2j}+\cdots+X_{ik}Y_{kj}.$$

由于矩阵 $X_{i\nu}, Y_{\nu j}$ 的阶所满足的条件，乘积 $X_{i\nu}Y_{\nu j}$ 也是有意义的. 矩阵的分块法即便在最简单的情况下也会带来方便，例如

$$\begin{pmatrix} E & A \\ 0 & E \end{pmatrix}\begin{pmatrix} A & 0 \\ -E & B \end{pmatrix} = \begin{pmatrix} 0 & AB \\ -E & B \end{pmatrix},$$

此处 $A, B, E, 0 \in M_n(\mathbb{R})$($E$ 是单位矩阵，0 是零矩阵).

18．令矩阵

$$X = (x_{ij}) \in M_n(\mathbb{R}), \qquad T = (t_{ij}) \in M_n(\mathbb{R}).$$

证明 T 左乘 X 得到行 $X_{(1)}, \cdots, X_{(n)}$ 的线性组合，而右乘得到列 $X^{(1)}, \cdots X^{(n)}$ 的线性组合，特别注意到如果

$$T = \begin{pmatrix} 1 & t_{12} & t_{13} & \cdots & t_{1n} \\ & 1 & t_{23} & \cdots & t_{2n} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix}$$

是上三角矩阵，则

$$TX = \begin{pmatrix} X_{(1)} + t_{12}X_{(2)} + \cdots + t_{1n}X_{(n)} \\ X_{(2)} + \cdots + t_{2n}X_{(n)} \\ \cdots \\ X_{(n)} \end{pmatrix}$$

是从 X 经过一系列 (II) 型初等行变换得到的矩阵.

第 3 章　行　列　式

第 1 章 §4 的公式 (3) 和 (9) 给出了当 $n=2,3$ 时未知数与方程个数均为 n 的线性方程组的解，这使人想到对于任意自然数 n, 类似的求解公式是否存在的问题.

归根结底，我们需要的是对所论公式中分子和分母的正确解释. 我们将说明怎样将它们看作从 n 阶方阵的集合到实数集 $\mathbb{R}$ 的一个 “通用” 函数 $\det: M_n(\mathbb{R}) \to \mathbb{R}$ 的值. 函数 det(行列式) 的有效构造也将给出对第 2 章提出的其他许多有关矩阵问题的回答. 事实上，行列式理论在数学中的作用远比我们涉及的问题广泛，并且这一理论的每一种应用都引出了行列式自身的构造方法. 其中最自然的方法之一是几何方法，它基于 “矩阵行列式与多维图形体积” 以及外 n 形式的类比. 因为需要更多的技巧，故而我们将采用 “分析” 方法，仅在开始时借助于几何直观.

§1　行列式：构造和基本性质

1. 几何背景　在引入行列式的一般概念之前，暂时忘记我们的任务，先来计算最简单的几何图形 —— 平行六面体的体积. n 阶方阵 $A=(a_{ij})$ 对应于一个平行六面体

$$\prod(A)=\prod(A^{(1)},A^{(2)},\cdots,A^{(n)}),$$

它的边由矩阵的列 $A^{(1)},A^{(2)},\cdots,A^{(n)}$, 即向量 (或点) $A^{(j)}=[a_{1j},a_{2j},\cdots,a_{nj}]\in\mathbb{R}^n$ 给出. $\Pi(A)$ 可以看作是 $\mathbb{R}^n$ 中的一个子集，由形如

$$x_1A^{(1)}+\cdots+x_nA^{(n)},\quad 0\leqslant x_i\leqslant 1$$

的点组成 (在具有直角坐标系的空间中，我们将列向量及其端点视为同一). 当 $n=1$ 时，平行六面体叫作线段，而 $n=2$ 时叫作平行四边形.

n 维平行六面体的体积 $v(\Pi(A))$ 由归纳法定义为它在 $\mathbb{R}^{n-1}$ 中的 $(n-1)$ 维底边的体积 $v(\Pi(A^{(1)},\cdots,A^{(n-1)}))$ 与点 $A^{(n)}$ 到底边所在超平面的垂线段的长度 h 的乘积. 例如线段 $(n=1)$ 的体积是它的长度，平行四边形 $(n=2)$ 的体积是它的面积. 我们现在不讨论度量体积的一般理论.

直接计算表明，不计符号

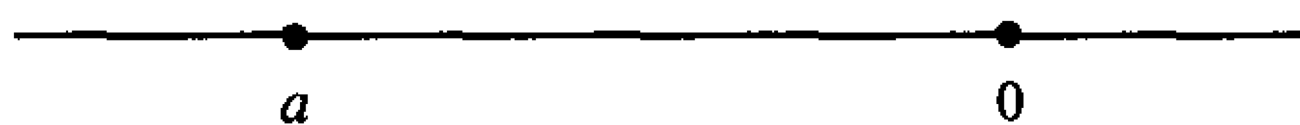
$$n=2: \quad v\left(\prod(A^{(1)},A^{(2)})\right)=\begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix};$$

$$n=3: \quad v\left(\prod(A^{(1)},A^{(2)},A^{(3)})\right)=\begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} \tag{1}$$

(2 阶和 3 阶矩阵的行列式由第 1 章 §4 公式 (2) 和 (8) 给出).

对于任意排列的多个点 $A^{(1)},A^{(2)},\cdots$，无条件地保留形如 (1) 的公式是一件诱人的事情，如果运用 **有向体积** 的概念，允许平行六面体的体积取负值，这件事就有可能实现.

例如当 $n=1$ 时，线段



的有向长度取 $a<0$. 当 $n=2$ 时若有序向量 $(A^{(1)},A^{(2)})$ 与基向量 (e_1,e_2) 在平面 $\mathbb{R}^2$ 上的定向一致，平行六面体 $\Pi(A^{(1)},A^{(2)})$ 的面积取正号，否则取负号. 在这样的意义之下，自然导出了公式 (1), 且任意 n 阶矩阵 A 的行列式 $|A|$ 可看作平行六面体的有向体积，记作:

$$\det A = v\left(\prod(A)\right).$$

与标准列 $E^{(j)}=[0,\cdots,1,\cdots,0]$ 相应的基向量 e_j 使得

$$A^{(j)}=\varphi_A(E^{(j)}),$$

它是基向量 e_j 在线性变换 $\varphi_A: X\to AX$ 之下的像 (见第 2 章 §3). 故平行六面体 $\Pi(A)$ 是单位立方体 $\Pi(E)$ 在线性映射 φ_A 之下的像，而因为 $v(\Pi(E))=1$, 行列式 $\det\varphi_A=\det A$ 等于有向体积的变换系数. 事实上，应用 φ_A, 可以将任意图形的有向体积，不仅是单位立方体，转化为 $\det A$(见 [BAII]).

现在我们易于列出检验的平行四边形有向面积的一些性质:

1) $v(\Pi(A^{(1)},A^{(2)}))=-v(\Pi(A^{(2)},A^{(1)}))$;

2) $v(\Pi(A^{(1)}+\lambda A^{(2)},A^{(2)}))=v(\Pi(A^{(1)},A^{(2)}))$;

3) $v(\Pi(E))=1$.

性质 1) 和 3) 前面已谈到过，性质 (2)(当 $n=2$ 时) 的图解见图 14, 它基于三角形的全等. 当 $n>3$ 时，平行六面体体积的性质 1)—3) 不是非常直观，然而无论从任何途径引入行列式理论，都应当满足上述三条性质，这一事实是完全清楚的.

此外，我们还需要得到行列式的其他一些性质，比如用于对任意给定的方阵 A 计算 $\det A$，从而计算 $v(\Pi(A))$，它们在算法上是可行的且易于实现的.

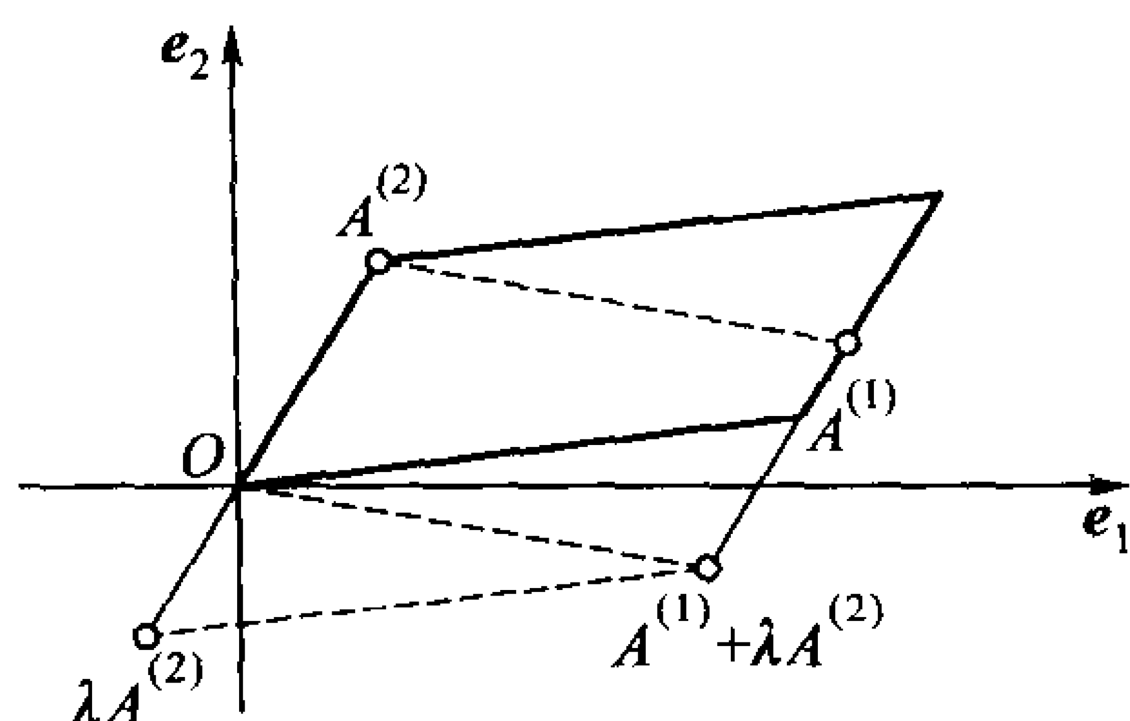


图 14

2. 组合 – 解析方法 两个外观相近的符号

$$A=\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix}, \qquad \det A=\begin{vmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{vmatrix} \tag{2}$$

对于我们并不陌生，我们以后将经常地使用这两个有本质区别的符号. 其中若 A 是一个填写了系数 (通常为数) 的正方形表格，那么这个表格的 n 阶行列式以两条垂直线为界，它是一个属于矩阵 A 的数 (或表达式)，由下述的 *完全展开式* 定义：

$$\det A=\sum_{\sigma\in S_n}\varepsilon_\sigma a_{1\sigma(1)}\, a_{2\sigma(2)}\cdots a_{n\sigma(n)}. \tag{3}$$

换言之，矩阵 $A=(a_{ij})$ 的 **行列式** $\det A$ 是取自不同行，不同列的系数 a_{ij} 的所有可能乘积的代数和. 在每一个乘积中，因子按照行脚标的顺序书写，而列脚标由行脚标在置换 $\sigma\in S_n$ 中的像 $\sigma(1),\sigma(2),\cdots,\sigma(n)$ 确定. 在这种记法下，和式 (3) 中共有 $n!$ 项；对应偶置换的各项取正号，而对应奇置换的各项取负号. 两种加项的个数相等，均为 $n!/2$，与第 1 章 §8 的关系式 (11) 一致.

简单的验算表明，当 $n=2$ 和 $n=3$ 时，公式 (3) 与我们已知的表达式相同. 设 $n=4$ 且 $\sigma=(1\,2)(3\,4)$. 则 $\varepsilon_\sigma=1$，而 $a_{1,\sigma(1)}a_{2,\sigma(2)}a_{3,\sigma(3)}a_{4,\sigma(4)}=a_{12}a_{21}a_{34}a_{43}$. 这就表明，在四阶行列式中，加项 $a_{12}a_{21}a_{34}a_{43}$ 取正号. 仔细地写出 4 阶行列式的全部 24 项，并注意观察符号的分布是一个有益的练习，可以导致对第 1 章 §8 内容的切实掌握. 当 $n=5$ 时写出 5 阶行列式 120 项的练习看来不是十分必要. 根据第 1 段的看法，我们希望作为出发点的公式 (3) 可以对任意阶行列式提炼出我们需要的所有的性质.

3. 行列式的基本性质 行列式的性质不多，但是为了表述，主要是为了理解它们，需要约定一些术语和符号.

以后我们沿用第 2 章的符号体系，用

$$A_{(i)}=(a_{i1},a_{i2},\cdots,a_{in}),\qquad i=1,2,\cdots,n,$$
$$A^{(j)}=[a_{1j},a_{2j}\cdots,a_{nj}],\qquad j=1,2,\cdots,n,$$

分别表示矩阵 $A=(a_{ij})$ 的第 i 行和第 j 列. 矩阵 A 本身既可以写成以行为元素的矩阵

$$A=[A_{(1)},A_{(2)},\cdots,A_{(n)}]$$

(即各行排成的一列), 亦可写成以列为元素的矩阵:

$$A=(A^{(1)},A^{(2)},\cdots,A^{(n)})$$

(即各列排成的一行). 我们约定，以后也可以将 $n\times n$ 矩阵 A 的行和列称为 n 阶行列式 $|a_{ij}|$ 的行和列.

根据定义，$||$=det(determinant 的缩写) 是一个函数，它把方阵 A 对应到一个数 $|A|=\det A$, 我们的任务是研究当改变矩阵 A 的行和列时，这个函数如何变化，这里将行和列看作线性空间 $\mathbb{R}^n$ 中的元素 (向量). 如果需要， $\det A$ 可简记作 n 个变量的函数 $\det[A_{(1)},\cdots,A_{(n)}]$(见第 1 章 §5 第 2 段), 或者 $\det(A^{(1)},\cdots,A^{(n)})$, 变量是 $\mathbb{R}^n$ 中的向量.

一个函数 $\mathcal{D}:[A_{(1)},\cdots,A_{(n)}]\mapsto\mathcal{D}(A_{(1)},\cdots,A_{(n)})$ 叫作 **多重线性的**, 如果它在每一个分量 $A_{(i)}$ 上都是线性的，也就是说

$$\begin{aligned}&\mathcal{D}(A_{(1)},\cdots,\alpha A'_{(i)}+\beta A''_{(i)},\cdots,\quad A_{(n)})\\&\quad=\alpha\mathcal{D}(A_{(1)},\cdots,A'_{(i)},\cdots,A_{(n)})+\beta\mathcal{D}(A_{(1)},\cdots,A''_{(i)},\cdots,A_{(n)})\end{aligned}$$

(与第 2 章 §3 的第 1 段比较). 如果

$$\begin{aligned}&\mathcal{D}(A_{(1)},\cdots,A_{(i)},A_{(i+1)},\cdots,A_{(n)})\\&\quad=-\mathcal{D}(A_{(1)},\cdots,A_{(i+1)},A_{(i)},\cdots,A_{(n)}),1\leqslant i\leqslant n-1,\end{aligned}\tag{4}$$

则称函数 $\mathcal{D}$ 为 **斜对称的**(见第 1 章 §8 第 4 段).

注记 1 从线性函数的定义 (见第 2 章 §3(4)) 可知, 函数 $\mathcal{D}$ 是多重线性的, 当且仅当对于固定的 $A_{(1)},\cdots,A_{(i-1)},A_{(i+1)},\cdots,A_{(n)}$ 以及 $A_{(i)}=X=(x_1,\cdots,x_n)$, 我们有

$$\mathcal{D}(A_{(1)},\cdots,A_{(n)})=\alpha_1x_1+\alpha_2x_2+\cdots+\alpha_nx_n,$$

其中 $\alpha_1,\cdots,\alpha_n$ 是不依赖于 $x_1,\cdots,x_n$ 的纯量.

注记 2 多重线性函数 $\mathcal{D}$ 的斜对称性等价于 $\mathcal{D}$ 满足关系式

$$\mathcal{D}(A_{(1)},\cdots,A_{(i-1)},X,X,A_{(i+2)},\cdots,A_{(n)})=0,\ 1\leqslant i\leqslant n-1.\tag{4'}$$

事实上，在 (4) 中取 $A_{(i)} = A_{(i+1)} = X$, 我们得到 (4′), 反之，取 $X = A_{(i)} + A_{(i+1)}$, 由于 $\mathcal{D}$ 的多重线性性，(4′) 导出了关系式

$$\begin{aligned}&\mathcal{D}(\cdots, A_{(i)}, A_{(i)}, \cdots) + \mathcal{D}(\cdots, A_{(i+1)}, A_{(i+1)}, \cdots)\\&\quad + \mathcal{D}(\cdots, A_{(i)}, A_{(i+1)}, \cdots) + \mathcal{D}(\cdots, A_{(i+1)}, A_{(i)}, \cdots)\\&= \mathcal{D}(\cdots, A_{(i)} + A_{(i+1)}, A_{(i)} + A_{(i+1)}, \cdots) = 0.\end{aligned}$$

式中的前两项为零 (在 (4′) 中分别取 $X = A_{(i)}$ 和 $X = A_{(i+1)}$ 即可), 所以后两项的和为零，得到关系式 (4).

同样的定义和讨论亦适用于列向量函数 $\mathcal{D}(A^{(1)}, \cdots, A^{(n)})$. 更一般地，斜对称性条件 (4) 适用于任意函数 $\mathcal{D}: M^n \to \mathbb{R}$, 其中 M^n 是集合 M 的笛卡儿幂，我们再一次指出，根据第 1 章引理 2, 当交换两个自变量的位置时，斜对称函数变号.

注意到在公式 (3) 中，矩阵 A 的行与列的地位乍看起来是不平等的. 但如果交换 A 的行和列，则有转置矩阵 ${}^tA$(见第 2 章 §3, 第 3 段). 因而要进行一下两个值 $\det A$ 和 $\det {}^tA$ 的比较. 答案由定理 1 给出.

定理 1 *任意方阵 A 及其转置 ${}^tA$ 的行列式相等：*

$$\det {}^tA = \det A.$$

证明 令 $A = (a_{ij}), {}^tA = (a'_{ij})$, 此处 $a'_{ij} = a_{ji}$. 并注意到对任意数码 $k \in \{1, 2, \cdots, n\}$ 和任意置换 $\pi \in S_n, k = \pi(\pi^{-1}k)$, 我们发现乘积 $a'_{1,\pi(1)} \cdots a'_{n,\pi(n)}$ 中的有序因子在置换 π^{-1} 的作用下给出

$$\begin{aligned}&a'_{\pi^{-1}(1),\pi^{-1}(\pi(1))} \cdots a'_{\pi^{-1}(n),\pi^{-1}(\pi(n))} = a'_{\pi^{-1}(1),1} \cdots a'_{\pi^{-1}(n),n}\\&= a_{1\pi^{-1}(1)} \cdots a_{n\pi^{-1}(n)}.\end{aligned}$$

如果再考虑到 $\varepsilon_\pi = \varepsilon_{\pi^{-1}}$,(事实上 $\varepsilon_\pi \cdot \varepsilon_{\pi^{-1}} = \varepsilon_{\pi\pi^{-1}} = \varepsilon_e = 1$), 而 $\{\pi^{-1} | \pi \in S_n\} = \{\pi | \pi \in S_n\} = S_n$(因为 $\pi \mapsto \pi^{-1}$ 是从 S_n 到自身的一个一一映射), 那么根据公式 (3) 有

$$\begin{aligned}\det {}^tA &= \sum_{\pi \in S_n} \varepsilon_\pi \, a'_{1,\pi(1)} \cdots a'_{n,\pi(n)} = \sum_{\pi \in S_n} \varepsilon_{\pi^{-1}} \, a'_{\pi^{-1}(1),1} \cdots a'_{\pi^{-1}(n),n}\\&= \sum_{\sigma \in S_n} \varepsilon_\sigma \, a_{1,\sigma(1)} \cdots a_{n,\sigma(n)} = \det A.\end{aligned}$$

□

注记 3 定理 1 的论断表明，如果行列式满足某种相对于行 (或列) 的性质，那么该性质相对于列 (或行) 也被满足.

定理 2 *定义在集合 $M_n(\mathbb{R})$ 上的函数 $\det : A \mapsto \det A$ 具有下述性质.*

D1. $\det A$ 是矩阵 A 的行的斜对称函数 (即交换任意两行时，行列式变号).

D2. $\det A$ 是矩阵 A 的行的多重线性函数 (即矩阵 A 的行列式是它的任意一行 $A_{(k)}$ 的元素的线性函数).

D3. $\det E = 1$.

证明 D1. 设 A' 是由 A 交换行 $A_{(s)}, A_{(t)}$ 得到的矩阵，也就是说 $A'_{(s)} = A_{(t)}$, $A'_{(t)} = A_{(s)}, A'_{(i)} = A_{(i)}$ 若 $i \neq s, t$. 将任意置换 $\pi \in S_n$ 写成 $\pi = \sigma\tau$ 的形式，其中 $\tau = (st)$ 是一个对换 (见第 1 章 §8 第 3 段公式 (10′) 关于置换 R_τ 的确定), 我们有

$$\begin{aligned}
\det A' &= \sum_{\pi \in S_n} \varepsilon_\pi \, a'_{1,\pi(1)} \cdots a'_{n,\pi(n)} \\
&= \sum_{\sigma \in S_n} \varepsilon_{\sigma\tau} \, a'_{1,\sigma\tau(1)} \cdots a'_{s,\sigma\tau(s)} \cdots a'_{t,\sigma\tau(t)} \cdots a'_{n,\sigma\tau(n)} \\
&= \sum_{\sigma \in S_n} \varepsilon_{\sigma\tau} \, a'_{1,\sigma(1)} \cdots a'_{s,\sigma(t)} \cdots a'_{t,\sigma(s)} \cdots a'_{n,\sigma(n)} \\
&= \sum_{\sigma \in S_n} \varepsilon_{\sigma\tau} \, a_{1,\sigma(1)} \cdots a_{t,\sigma(t)} \cdots a_{s,\sigma(s)} \cdots a_{n,\sigma(n)} \\
&= -\sum_{\sigma \in S_n} \varepsilon_\sigma \, a_{1,\sigma(1)} \cdots a_{n,\sigma(n)} = -\det A.
\end{aligned}$$

D2. 设 $A = (a_{ij})$, 并设 $A_{(k)} = \lambda' A'_{(k)} + \lambda'' A''_{(k)}$, 其中撇号指出了辅助矩阵

$$\begin{aligned}
A' &= [A_{(1)}, \cdots, A_{(k-1)}, \ A'_{(k)}, A_{(k+1)}, \cdots, A_{(n)}], \\
A'' &= [A_{(1)}, \cdots, A_{(k-1)}, \ A''_{(k)}, A_{(k+1)}, \cdots, A_{(n)}].
\end{aligned}$$

根据条件

$$a_{kj} = \lambda' a'_{kj} + \lambda'' a''_{kj}, \quad j = 1, 2, \cdots, n.$$

基于注记 1,$\det A$ 关于第 k 行 $A_{(k)}$ 的元素的线性可以给出下述论断. 由定义

$$\begin{aligned}
&\det[A_{(1)}, \cdots, A_{(k)}, \cdots, A_{(n)}] = \det A \\
&= \sum_{\sigma \in S_n} \varepsilon_\sigma a_{1,\sigma(1)} \cdots a_{k,\sigma(k)} \cdots a_{n,\sigma(n)} = \sum_{\sigma \in S_n} p_\sigma a_{k,\sigma(k)},
\end{aligned}$$

其中 $p_\sigma, \sigma \in S_n$, 是系数，它不依赖于行 $A_{(k)}$ 的元素. 将脚标满足 $\sigma(k) = j, \sigma \in S_n$, 的 p_σ 合并同类项，并设 $\alpha_j = \sum\limits_{\sigma(k)=j} p_\sigma$, 我们就得到了所需的线性

$$\det[\cdots, A_{(k)}, \cdots] = \sum_{j=1}^{n} \alpha_j a_{kj},$$

$$\begin{aligned}
\det[\cdots, \lambda' A'_{(k)} + \lambda'' A''_{(k)}, \cdots] &= \sum_{j=1}^{n} \alpha_j (\lambda' a'_{kj} + \lambda'' a''_{kj}) \\
&= \lambda' \sum_{j=1}^{n} \alpha_j a'_{kj} + \lambda'' \sum_{j=1}^{n} \alpha_j a''_{kj} \\
&= \lambda' \det[\cdots, A'_{(k)}, \cdots] + \lambda'' \det[\cdots, A''_{(k)}, \cdots].
\end{aligned}$$

简言之：

$$\det A = \lambda' \det A' + \lambda'' \det A''.$$

D3. 显然，
$$\det E = \sum_{\sigma\in S_n} \varepsilon_\sigma \delta_{1,\sigma(1)}\cdots\delta_{n,\sigma(n)} = \varepsilon_e\delta_{1,1}\cdots\delta_{n,n} = 1.$$
□

定理 2 蕴含着几个简单的结论，我们简述为行列式的性质，但我们将在更广泛的情况下，对具有性质 D1~D2 的任意函数 $D: M_n(\mathbb{R}) \to \mathbb{R}$ 进行证明.

D4. 设 $A \in M_n(\mathbb{R}), \lambda \in \mathbb{R}$. 则

$$\det \lambda A = \lambda^n \det A.$$

证明 对下标为 $1, 2, \cdots$ 的行依次运用性质 D2, 我们有

$$\begin{aligned}\mathcal{D}(\lambda A) &= \mathcal{D}[\lambda A_{(1)}, \lambda A_{(2)}, \cdots, \lambda A_{(n)}] = \lambda\mathcal{D}[A_{(1)}, \lambda A_{(2)}, \cdots, \lambda A_{(n)}] \\ &= \lambda^2\mathcal{D}[A_{(1)}, A_{(2)}, \cdots, \lambda A_{(n)}] = \cdots = \lambda^n\mathcal{D}[A_{(1)}, A_{(2)}, \cdots, A_{(n)}] \\ &= \lambda^n\mathcal{D}(A).\end{aligned}$$
□

D5. *有一行为零的行列式等于 0.*

证明 设 $A_{(k)} = (0, 0, \cdots, 0)$, 那么也有 $2A_{(k)} = (0, 0, \cdots, 0)$. 根据 D2,

$$\begin{aligned}\mathcal{D}(A) &= \mathcal{D}[A_{(1)}, \cdots, A_{(k)}, \cdots, A_{(n)}] \\ &= \mathcal{D}[A_{(1)}, \cdots, 2A_{(k)}, \cdots, A_{(n)}] \\ &= 2\mathcal{D}[A_{(1)}, \cdots, A_{(k)}, \cdots, A_{(n)}] = 2\mathcal{D}(A),\end{aligned}$$

从而 $\mathcal{D}(A) = 0$. □

D6. *如果在方阵 A 中有两行相同，则 A 的行列式等于 0.*

证明 取满足性质 D1~D2 的任意函数 $\mathcal{D}$. 在 A 中交换两个彼此相同的行 $A_{(s)}, A_{(t)}$, 我们仍然得到矩阵 A. 另一方面，由于 $\mathcal{D}$ 满足性质 D1,$\mathcal{D}(A)$ 的值变号. 这样 $\mathcal{D}(A) = -\mathcal{D}(A)$, 从而 $2\mathcal{D}(A) = 0, \mathcal{D}(A) = 0$. □

D7. *如果对行列式的行施行 (II) 型初等变换，其值不变.*

证明 考察施行一次初等变换的情况就足够了. 设矩阵 A' 是由矩阵 A 的第 t 行乘以 λ 加到第 s 行上得到的. 由于 $\mathcal{D}$ 的性质 D1 和 D6, 我们有

$$\begin{aligned}\mathcal{D}(A') &= \mathcal{D}(A_{(1)}, \cdots, A_{(s)} + \lambda A_{(t)}, \cdots, A_{(n)}) \\ &= \mathcal{D}(\cdots, A_{(s)}, \cdots) + \lambda\mathcal{D}(\cdots, A_{(t)}, \cdots, A_{(t)}, \cdots) \\ &= \mathcal{D}(A_{(1)}, \cdots, A_{(n)}) \\ &= \mathcal{D}(A).\end{aligned}$$
□

注记 4 上述证明说明，满足性质 D1~D2 的任意函数 $\mathcal{D}: M_n(\mathbb{R}) \to \mathbb{R}$ 亦满足性质 D4—D7 (将记号 det 换成 $\mathcal{D}$).

命题 1 设

$$\bar{A}=\begin{pmatrix}\bar{a}_{11} & \bar{a}_{12} & \cdots & \bar{a}_{1n}\\ 0 & \bar{a}_{22} & \cdots & \bar{a}_{2n}\\ \cdots & \cdots & \cdots & \cdots\\ 0 & 0 & \cdots & \bar{a}_{nn}\end{pmatrix} \tag{5}$$

是一个 n 阶上三角矩阵，E 是单位矩阵，且 $\mathcal{D}: M_n(\mathbb{R}) \to \mathbb{R}$ 是满足性质 D1~D2 的任意函数. 则

$$\mathcal{D}(\bar{A})=\mathcal{D}(E)\bar{a}_{11}\bar{a}_{22}\cdots\bar{a}_{nn}.$$

证明 根据注记 4, 我们可以运用性质 D2 和 D7. 根据 D2, 将 $\bar{a}_{nn}$ 移到符号 $\mathcal{D}$ 外：

$$\mathcal{D}(\bar{A})=\bar{a}_{nn}\mathcal{D}(\begin{pmatrix}\bar{a}_{11} & \cdots & \bar{a}_{1,n-1} & \bar{a}_{1n}\\ \cdots & \cdots & \cdots & \cdots\\ 0 & \cdots & \bar{a}_{n-1,n-1} & \bar{a}_{n-1,n}\\ 0 & \cdots & 0 & 1\end{pmatrix}).$$

现在对 $\bar{A}$ 施行 (II) 型初等变换，从符号 $\mathcal{D}$ 内矩阵的第 i 行减去最后一行与 $\bar{a}_{in}$ 的乘积. 这时最后一列的元素变为零 (除 $\bar{a}_{nn}=1$)，而矩阵中所有其他的元素保持不变. 对所得矩阵的倒数第二行施行同样的论证，等等. 依序施行一次，元素 $\bar{a}_{ii}$ 提到符号 $\mathcal{D}$ 之前，论证重新开始. 施行 n 次之后，我们确定

$$\mathcal{D}(\bar{A})=\bar{a}_{nn}\cdots\bar{a}_{11}\cdot\mathcal{D}(\begin{pmatrix}1 & \cdots & 0\\ \cdots & \cdots & \cdots\\ 0 & \cdots & 1\end{pmatrix}),$$

即为所求. □

推论 如果 $\bar{A}$ 是形如 (5) 式的矩阵，则

$$\det\bar{A}=\bar{a}_{11}\bar{a}_{22}\cdots\bar{a}_{nn}. \tag{6}$$

证明 因为 $\det E=1$(性质 D3), 推论直接由命题 1 得到. □

公式 (6) 也可以从后面更一般的结论得到. 先给出下述

定义 从矩阵 $A=(a_{ij})$ 中去掉第 i 行和第 j 列得到的矩阵的行列式记作 M_{ij}，称为矩阵 A 的对应于元素 a_{ij} 的 **子式**. 数值 $A_{ij}=(-1)^{i+j}M_{ij}$ 叫作元素 a_{ij} 的 **代数余子式**.

命题 2 若

$$A=\begin{pmatrix}a_{11} & a_{12} & \cdots & a_{1n}\\ 0 & a_{22} & \cdots & a_{2n}\\ \cdots & \cdots & \cdots & \cdots\\ 0 & a_{n2} & \cdots & a_{nn}\end{pmatrix},$$

则

$$\det A = a_{11}M_{11} = a_{11}A_{11}.$$

证明 因为 $\det A = \det {}^tA$(定理 1), 又因为 a_{11} 是第一列 $A^{(1)}$ 中唯一的非零元素，故当 $\pi(1) \neq 1$ 时， $a_{\pi(1),1} = 0$, 且

$$\det A = \sum_{\pi \in S_n} \varepsilon_\pi a_{\pi(1),1} a_{\pi(2),2} \cdots a_{\pi(n),n} = \sum_{\pi \in S_n, \pi(1)=1} \varepsilon_\pi a_{1,1} a_{\pi(2),2} \cdots a_{\pi(n),n}.$$

保留第 1 个元素 1 不动的置换 $\pi \in S_n$ 的集合与作用在 $\{2, 3, \cdots, n\}$ 上的置换的集合 S_{n-1} 重合. 这样,

$$\begin{aligned}\det A &= a_{11} \sum_{\sigma \in S_{n-1}} \varepsilon_\sigma \, a_{\sigma(2),2} \cdots a_{\sigma(n),n} \\ &= a_{11} \begin{vmatrix} a_{22} & \cdots & a_{2n} \\ \cdots & \cdots & \cdots \\ a_{n2} & \cdots & a_{nn} \end{vmatrix} = a_{11}M_{11}.\end{aligned}$$ □

将命题 2 应用于上三角矩阵 $\bar{A}$, 得到等式 $\det \bar{A} = \bar{a}_{11}\overline{M}_{11}$, 其中

$$\overline{M}_{11} = \begin{vmatrix} \bar{a}_{22} & & * \\ & \ddots & \\ 0 & & \bar{a}_{nn} \end{vmatrix}$$

是阶数比 $\det \bar{A}$ 少 1 的同类型的行列式. 显然由归纳法可得公式 (6).

上述性质提供了较简单地计算 n 阶行列式的可能性. 方法之一如下. 将矩阵 $A = (a_{ij})$ 用初等变换化为上三角形 (见第 1 章 §3). 得到了形如 (5) 的矩阵 $\bar{A}$. 假设在过程中完成了 q 次 (I) 型初等变换和若干次 (Ⅱ) 型初等变换. 由于后者不改变行列式的值 (D7), 而每一个 (I) 型初等变换将行列式变号 (乘以 (-1)), 故 $\det \bar{A} = (-1)^q \det A$. 由公式 (6), 我们有

$$\det \bar{A} = \bar{a}_{11}\bar{a}_{22} \cdots \bar{a}_{nn}.$$

这时

$$\det A = (-1)^q \bar{a}_{11}\bar{a}_{22} \cdots \bar{a}_{nn}. \tag{7}$$

得到计算 $\det A$ 的一种公式.

现在我们来根据公式 (7) 说明行列式的性质 D1—D3 所起的作用.

定理 3 设 $\mathcal{D} : M_n(\mathbb{R}) \to \mathbb{R}$ 是具有下列性质的函数:

i) 当交换矩阵 $A \in M_n(\mathbb{R})$ 的任意相邻两行时，$\mathcal{D}(A)$ 变号;

ii) $\mathcal{D}(A)$ 是 A 的每一行的线性函数 (换言之，$\mathcal{D}(A)$ 是矩阵的行的斜对称多重线性函数).

则

$$\mathcal{D}(A) = \mathcal{D}(E) \cdot \det A.$$

证明　我们知道，性质 i) 等价于说，当交换任意两行时，即在任意 (I) 型初等变换下，$\mathcal{D}(A)$ 变号. 根据注记 4, $\mathcal{D}(A)$ 具有性质 D4—D7. 特别地，$\mathcal{D}(A)$ 的值在矩阵 A 的行经过 (II) 型初等变换后不变.

借助初等变换将矩阵 A 化为上三角形 (5), 其中某些 $\bar{a}_{ii}$ 可能等于零. 考虑到前面的事实，我们有公式 (见 (7))

$$\det A = (-1)^q \det \bar{A} = (-1)^q \bar{a}_{11}\ \bar{a}_{22} \cdots \bar{a}_{nn},$$
$$\mathcal{D}(A) = (-1)^q \mathcal{D}(\bar{A}),$$

其中 q 是从 A 到 $\bar{A}$ 所做的 (I) 型初等变换的个数. 关系式 $\mathcal{D}(A) = \mathcal{D}(E) \det A$ 现在可以直接从命题 1 得出.　□

由此可见，函数 det 的性质 D1—D3 唯一地刻画了这个函数. 基于这一理由，我们将它们列为行列式的基本性质. 从一开始就把具有性质 D1—D3 的函数 $\mathcal{D}$ 叫作行列式也是可以的，但在那种情况下就必须证明它的存在性. 对于我们来说，存在性是由函数 det 自身的构造 —— 公式 (3) 保证了的.

考虑到定理 3 今后的应用，我们没有在定理的叙述中加入规范化条件 $\mathcal{D}(E) = 1$.

习　题

1. 将下述三个变量的斜对称函数 $\Delta : \mathbb{R}^3 \to \mathbb{R}$

$$\Delta(x, y, z) = (y - x)(z - x)(y - z)$$

写成三阶行列式的形式.

2. 设 $A = (a_{ij}), A' = (a'_{ij})$ 是两个 $n \times n$ 矩阵， Δ, Δ' 是它们的行列式. 在下述情况下比较 Δ 和 Δ':

a) $a'_{ij} = 2^{i-j} a_{ij}$;

b) $a'_{ij} = a_{n+1-i,j}$;

c) $a'_{ij} = a_{n+1-i,n+1-j}$.

3. 证明

$$\begin{vmatrix} 1 & 1 & 1 & \cdots & 1 & 1 \\ 1 & 2 & 1 & \cdots & 1 & 1 \\ 1 & 1 & 3 & \cdots & 1 & 1 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 1 & 1 & 1 & \cdots & n & 1 \\ 1 & 1 & 1 & \cdots & 1 & n+1 \end{vmatrix} = n!.$$

§2 行列式的进一步性质

1. 行列式按一行或一列的元素展开 有一种计算行列式的常用方法，基于逐次降低行列式的阶数. 它需要用到子式 M_{ij} 和代数余子式 A_{ij} 的概念 (见 §1 的定义).

定理 1 设 $A=(a_{ij})\in M_n(\mathbb{R})$. 下述公式成立：

$$\det A=\sum_{i=1}^{n}(-1)^{i+j}a_{ij}M_{ij}=\sum_{i=1}^{n}a_{ij}A_{ij} \tag{1}$$

(行列式按照第 j 列的元素展开);

$$\det A=\sum_{j=1}^{n}(-1)^{i+j}a_{ij}M_{ij}=\sum_{j=1}^{n}a_{ij}A_{ij} \tag{2}$$

(行列式按照第 i 行的元素展开).

换言之，矩阵 A 的行列式等于某列 (或某行) 的一切元素与它们的代数余子式的乘积之和.

证明 1) 根据基本性质 D1 和 D2, 行列式 (先对应于列，而后对应于行) 满足一系列等式：

$$\det A=\begin{vmatrix} a_{11} & \cdots & a_{1j} & \cdots & a_{1n}\\ a_{21} & \cdots & a_{2j} & \cdots & a_{2n}\\ \cdots & \cdots & \cdots & \cdots & \cdots\\ a_{n1} & \cdots & a_{nj} & \cdots & a_{nn}\end{vmatrix}$$

$$=\begin{vmatrix} a_{11} & \cdots & a_{1j} & \cdots & a_{1n}\\ a_{21} & \cdots & 0 & \cdots & a_{2n}\\ \cdots & \cdots & \cdots & \cdots & \cdots\\ a_{n1} & \cdots & 0 & \cdots & a_{nn}\end{vmatrix}+\begin{vmatrix} a_{11} & \cdots & 0 & \cdots & a_{1n}\\ a_{21} & \cdots & a_{2j} & \cdots & a_{2n}\\ \cdots & \cdots & \cdots & \cdots & \cdots\\ a_{n1} & \cdots & 0 & \cdots & a_{nn}\end{vmatrix}$$

$$+\cdots+\begin{vmatrix} a_{11} & \cdots & 0 & \cdots & a_{1n}\\ a_{21} & \cdots & 0 & \cdots & a_{2n}\\ \cdots & \cdots & \cdots & \cdots & \cdots\\ a_{n1} & \cdots & a_{nj} & \cdots & a_{nn}\end{vmatrix}$$

$$=\sum_{i=1}^{n}\begin{vmatrix} a_{11} & \cdots & a_{1,j-1} & 0 & a_{1,j+1} & \cdots & a_{1n}\\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots\\ a_{i1} & \cdots & a_{i,j-1} & a_{ij} & a_{i,j+1} & \cdots & a_{in}\\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots\\ a_{n1} & \cdots & a_{n,j-1} & 0 & a_{n,j+1} & \cdots & a_{nn}\end{vmatrix}$$

$$
= \sum_{i=1}^{n} (-1)^{j-1} \begin{vmatrix} 0 & a_{11} & \cdots & a_{1,j-1} & a_{1,j+1} & \cdots & a_{1n} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ a_{ij} & a_{i1} & \cdots & a_{i,j-1} & a_{i,j+1} & \cdots & a_{in} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & a_{n1} & \cdots & a_{n,j-1} & a_{n,j+1} & \cdots & a_{nn} \end{vmatrix}
$$

$$
= \sum_{i=1}^{n} (-1)^{(j-1)+(i-1)} \begin{vmatrix} a_{ij} & a_{i1} & \cdots & a_{i,j-1} & a_{i,j+1} & \cdots & a_{in} \\ 0 & a_{11} & \cdots & a_{1,j-1} & a_{1,j+1} & \cdots & a_{1n} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & a_{j-1,1} & \cdots & a_{j-1,j-1} & a_{j-1,j+1} & \cdots & a_{j-1,n} \\ 0 & a_{j+1,1} & \cdots & a_{j+1,j-1} & a_{j+1,j+1} & \cdots & a_{j+1,n} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & a_{n1} & \cdots & a_{n,j-1} & a_{n,j+1} & \cdots & a_{nn} \end{vmatrix}
$$

$$
= \sum_{i=1}^{n} (-1)^{i+j} a_{ij} M_{ij}.
$$

最后一个等式基于对矩阵 A' 使用 §1 命题 2,

$$
A' = \begin{pmatrix} a'_{11} & a'_{12} & \cdots & a'_{1n} \\ 0 & a'_{22} & \cdots & a'_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ 0 & a'_{n2} & \cdots & a'_{nn} \end{pmatrix},
$$

其中 $a'_{11} = a_{ij}, a'_{12} = a_{i1}, \cdots, a'_{1n} = a_{in}, M'_{11} = M_{ij}$. 回忆定义 $A_{ij} = (-1)^{i+j} M_{ij}$. 公式 (1) 得证.

2) 令 ${}^tA = (a'_{ji}), a'_{ji} = a_{ij}$. 我们再次指出, 对应于 $\det {}^tA$ 的元素 a'_{ji} 的子式为 $M'_{ji} = M_{ij}$. 用 1) 的结论, $\det A = \det {}^tA = \sum\limits_{j=1}^{n} (-1)^{j+i} a'_{ji} M'_{ji} = \sum\limits_{j=1}^{n} (-1)^{i+j} a_{ij} M_{ij}$, 公式 (2) 得证. 亦可直接引用 §1 注记 3 简单地证明. □

举两个例子用来说明行列式的上述性质.

例 1 行列式

$$
\Delta_n = \begin{vmatrix} 1 & 1 & \cdots & 1 \\ x_1 & x_2 & \cdots & x_n \\ x_1^2 & x_2^2 & \cdots & x_n^2 \\ \cdots & \cdots & \cdots & \cdots \\ x_1^{n-1} & x_2^{n-1} & \cdots & x_n^{n-1} \end{vmatrix} = \Delta(x_1, x_2, \cdots, x_n)
$$

叫作 **范德蒙德行列式**, 可按公式

$$
\Delta_n = \prod_{1 \leqslant i < j \leqslant n} (x_j - x_i) \tag{3}
$$

计算，或更详细地写成

$$\Delta_n=(x_2-x_1)(x_3-x_1)\cdots(x_n-x_1)(x_3-x_2)\cdots(x_n-x_2)\cdots(x_{n-1}-x_n)$$

(回顾 §1 习题 1 与这一公式的联系). 特别地，当元素 $x_1,\cdots,x_n$ 两两不同时，范德蒙德行列式不等于零. 它的这一性质经常被用到. 根据 §1 定理 1, 我们也有

$$\Delta_n=\begin{vmatrix}1 & x_1 & x_1^2 & \cdots & x_1^{n-1}\\ 1 & x_2 & x_2^2 & \cdots & x_2^{n-1}\\ \cdots & \cdots & \cdots & \cdots & \cdots\\ 1 & x_n & x_n^2 & \cdots & x_n^{n-1}\end{vmatrix}.$$

现在对 n 作归纳法来证明公式 (3). 假设当 $m<n$ 时，Δ_m 可由公式 (3) 计算，根据性质 D7, 对于每一个 i, 我们从行列式 Δ_n 的第 i 行减去第 $(i-1)$ 行乘以 x_1:

$$\Delta_n=\begin{vmatrix}1 & 1 & \cdots & 1\\ 0 & x_2-x_1 & \cdots & x_n-x_1\\ 0 & x_2^2-x_2x_1 & \cdots & x_n^2-x_nx_1\\ \cdots & \cdots & \cdots & \cdots\\ 0 & x_2^{n-1}-x_2^{n-2}x_1 & \cdots & x_n^{n-1}-x_n^{n-2}x_1\end{vmatrix}.$$

现在将行列式按照第一列的元素展开，并在所得到的 $(n-1)$ 阶行列式中将第 j 列 $(j=1,2,\cdots,n-1)$ 的公因子 $x_{j+1}-x_j$ 提到行列式符号的外面 (行列式关于列的性质 D1). 我们得到了表达式

$$\begin{aligned}\Delta_n&=(x_n-x_1)(x_{n-1}-x_1)\cdots(x_2-x_1)\begin{vmatrix}1 & 1 & \cdots & 1\\ x_2 & x_3 & \cdots & x_n\\ \cdots & \cdots & \cdots & \cdots\\ x_2^{n-2} & x_3^{n-2} & \cdots & x_n^{n-2}\end{vmatrix}\\ &=(x_n-x_1)(x_{n-1}-x_1)\cdots(x_2-x_1)\cdot\Delta(x_2,x_3,\cdots,x_n),\end{aligned}$$

由归纳条件对最后一个因子使用 (3) 式

$$\Delta(x_2,\cdots,x_n)=\prod_{2\leqslant i<j\leqslant n}(x_j-x_i).$$

例 2 形如

$$A=\begin{pmatrix}0 & a_{12} & a_{13} & \cdots & a_{1n}\\ -a_{12} & 0 & a_{23} & \cdots & a_{2n}\\ -a_{13} & -a_{23} & 0 & \cdots & a_{3n}\\ \cdots & \cdots & \cdots & \cdots & \cdots\\ -a_{1n} & -a_{2n} & -a_{3n} & \cdots & 0\end{pmatrix}$$

的矩阵 $A=(a_{ij})$ 叫作 **斜对称的**(其行列式亦称为 **斜对称的**). 换言之 ${}^tA=-A$, 考虑到 §1 的定理 1, 我们有

$$\det A=\det{}^tA=\det(-A)=(-1)^n\det A,$$

从而 $\left[1+(-1)^{n-1}\right]\det A=0$. 当 n 是奇数时, 得到 $\det A=0$, 即任意奇数阶斜对称矩阵的行列式等于零.

2. 特殊矩阵的行列式 如果矩阵 A 的元素中有较多的零, 并且它们的位置"较好", 那么计算行列式 $\det A$ 比较容易. 在某些情况下这样的直觉可以导致准确的公式. 例如我们知道 (见 §1(6) 式)(上或下) 三角矩阵的行列式等于主对角线上元素之积. 另一个重要的特殊情况是

定理 2 *设 $m+n$ 阶行列式 D 在前 n 列与后 m 行的交叉处为 0, 则有下述公式:*

$$\begin{vmatrix} a_{11} & \cdots & a_{1n} & a_{1,n+1} & \cdots & a_{1,n+m} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ a_{n1} & \cdots & a_{nn} & a_{n,n+1} & \cdots & a_{n,n+m} \\ 0 & \cdots & 0 & b_{11} & \cdots & b_{1m} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & \cdots & 0 & b_{m1} & \cdots & b_{mm} \end{vmatrix} = \begin{vmatrix} a_{11} & \cdots & a_{1n} \\ \cdots & \cdots & \cdots \\ a_{n1} & \cdots & a_{nn} \end{vmatrix} \cdot \begin{vmatrix} b_{11} & \cdots & b_{1m} \\ \cdots & \cdots & \cdots \\ b_{m1} & \cdots & b_{mm} \end{vmatrix}$$

(等式左边的行列式叫作 **准三角的** 或 **带有零角的** 行列式).

证明 首先固定 $n(n+m)$ 个元素 a_{ij}, 并将行列式 D 看作元素 b_{kl} 的函数, b_{kl} 组成一个 m 阶方阵 B. 因而所得函数可看作矩阵 B 的函数: $D=\mathcal{D}(B)$.

显然, 行列式 D 关于后 m 行的多重线性性质和斜对称性, 等价于 $\mathcal{D}(B)$ 关于 B 的行有同样的性质. 这就意味着将 §1 定理 3 应用于 $\mathcal{D}(B)$ 是合理的, 因此 $\mathcal{D}(B)=\mathcal{D}(E)\det B$. 根据函数 $\mathcal{D}$ 的定义, 我们有:

$$\mathcal{D}(E)=\begin{vmatrix} a_{11} & \cdots & a_{1n} & a_{1,n+1} & \cdots & a_{1,n+m} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ a_{n1} & \cdots & a_{nn} & a_{n,n+1} & \cdots & a_{n,n+m} \\ 0 & \cdots & 0 & 1 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & \cdots & 0 & 0 & \cdots & 1 \end{vmatrix}.$$

按照最后一行展开 $\mathcal{D}(E)$(见公式 (2)), 然后按倒数第二行展开等等. 重复这一算法 m 次, 我们得到 $\mathcal{D}(E)=\det A$, 其中

$$A=\begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \cdots & \cdots & \cdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix}.$$

最后有 $D = \mathcal{D}(B) = \det A \cdot \det B$. □

使用新符号可将定理 2 的公式写成更紧凑的形式

$$\det \begin{pmatrix} A & C \\ 0 & B \end{pmatrix} = \det A \cdot \det B, \tag{4}$$

其中 A, B 是方阵，而 0 和 C 是长方阵.

将 §1 的定理 1 和定理 2 结合起来，或使用定理 2 的证法直接论证，易得

$$\det \begin{pmatrix} A & 0 \\ C & B \end{pmatrix} = \det A \cdot \det B. \qquad \square$$

当我们试图写出行列式 $\det \begin{pmatrix} C & A \\ B & 0 \end{pmatrix}$ 的表达式时，旋即得到了一个简单的反例 $\begin{vmatrix} 0 & 1 \\ 1 & 0 \end{vmatrix} = -1$. 问题在于符号. 为了得到正确的结论，必须交换行或列，将矩阵 $\begin{pmatrix} C & A \\ B & 0 \end{pmatrix}$ 化成 $\begin{pmatrix} B & 0 \\ C & A \end{pmatrix}$ 或 $\begin{pmatrix} A & C \\ 0 & B \end{pmatrix}$ 的形式.

更简单的方法基于已使用过若干次的 §1 定理 3. 事实上

$$\det \begin{pmatrix} C & A \\ B & 0 \end{pmatrix} = \det \begin{pmatrix} C & A \\ E & 0 \end{pmatrix} \cdot \det B.$$

其次运用公式 (2)m 次，得到

$$\det \begin{pmatrix} C & A \\ E_m & 0 \end{pmatrix} = \begin{vmatrix} & & & a_{11} & \cdots & a_{1n} \\ & * & & \cdots & \cdots & \cdots \\ & & & a_{n1} & \cdots & a_{nn} \\ 1 & \cdots & 0 & 0 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & \cdots & 1 & 0 & \cdots & 0 \end{vmatrix}$$
$$= (-1)^{(n+2)+(n+4)+\cdots+(n+2m)} \det A = (-1)^{mn} \det A.$$

最后，如果 A, B 分别是 n, m 阶方阵，则

$$\det \begin{pmatrix} C & A \\ B & 0 \end{pmatrix} = (-1)^{nm} \det A \cdot \det B. \tag{5}$$

公式 (4) 和 (5) 包含在关于行列式展开的拉普拉斯一般定理中. 但这个定理的使用面较窄，我们就不再讨论了，留给好学的读者作为下一节后面的练习.

关于矩阵的行列式在理论方面最重要的论断是

定理 3　设 A 和 B 是 n 阶方阵, 则

$$\det AB = \det A \cdot \det B.$$

证明　根据第 2 章 §3 公式 (7) 和 (9), 可以将矩阵 $(c_{ij}) = AB = (a_{ij})(b_{ij})$ 的系数 c_{ij} 用矩阵 A 和 B 的系数表示出来, 第 i 行 $(AB)_{(i)}$ 写成下式

$$(AB)_{(i)} = (A_{(i)}B^{(1)}, A_{(i)}B^{(2)}, \cdots, A_{(i)}B^{(n)}),$$
$$A_{(i)}B^{(j)} = \sum_{k=1}^{n} a_{ik}b_{kj}.$$

固定矩阵 B, 任取矩阵 A, 令

$$\mathcal{D}_B(A) = \det AB.$$

我们证明, 函数 $\mathcal{D} = \mathcal{D}_B$ 满足 §1 定理 3 的条件 i),ii). 事实上, 将 $A_{(s)}$ 与 $A_{(t)}$ 交换位置. 由于矩阵 AB 的第 s 行和第 t 行形如

$$(A_{(s)}B^{(1)}, \cdots, A_{(s)}B^{(n)}),$$
$$(A_{(t)}B^{(1)}, \cdots, A_{(t)}B^{(n)}),$$

那么 $(AB)_{(s)}$ 与 $(AB)_{(t)}$ 也交换了位置, 于是根据定理 1,

$$\begin{aligned}&\mathcal{D}(\cdots, A_{(s)}, \cdots, A_{(t)}, \cdots) = \mathcal{D}(A)\\&= \det AB = \det[\cdots, (AB)_{(s)}, \cdots, (AB)_{(t)}, \cdots]\\&= -\det[\cdots, (AB)_{(t)}, \cdots, (AB)_{(s)}, \cdots]\\&= -\mathcal{D}(\cdots, A_{(t)}, \cdots, A_{(s)}, \cdots).\end{aligned}$$

进一步, $\det AB$ 是第 i 行 $(AB)_{(i)}$ 的元素的线性函数:

$$\det AB = \lambda_1 A_{(i)}B^{(1)} + \lambda_2 A_{(i)}B^{(2)} + \cdots + \lambda_n A_{(i)}B^{(n)}.$$

所以

$\mathcal{D}(A) = \sum_{j=1}^{n} \lambda_j \sum_{k=1}^{n} a_{ik}b_{kj} = \sum_{k=1}^{n} a_{ik} \sum_{j=1}^{n} \lambda_j b_{kj} = \sum_{k=1}^{n} \mu_k a_{ik}$, 其中 $\mu_k = \sum_{j=1}^{n} \lambda_j b_{kj}$ 是一个纯量, 它不依赖于矩阵 A 的第 i 行的元素.

我们看到 $\mathcal{D}$ 对矩阵 A 的第 i 行的元素是线性的.

这样, §1 定理 3 的两个条件皆满足, 故 $\mathcal{D}(A) = \mathcal{D}(E) \cdot \det A$. 但是根据定义 $\mathcal{D}(E) = \det EB = \det B$. 所求公式得证. □

当 $n = 2$ 时, 定理 3 容易直接验证, 但当 $n = 3$ 时, 直接计算已经非常困难. 然而在一般情况下, 可以采用迂回手段, 直接运用性质 D1~D2, 或运用定理 2(见习题 3).

习 题

1. 整数 1798, 2139, 3255, 4867 可以被 31 整除. 不必计算, 证明 4 阶行列式

$$\begin{vmatrix} 1 & 7 & 9 & 8 \\ 2 & 1 & 3 & 9 \\ 3 & 2 & 5 & 5 \\ 4 & 8 & 6 & 7 \end{vmatrix}$$

也可以被 31 整除.

2. 证明任意四阶斜对称行列式 $|a_{ij}|$, 其中 $a_{ij} \in \mathbb{Z}$, 是一个整数的平方.

注记 这对于任意阶的斜对称行列式都是对的.

3. 用下述方法证明 $\det AB = \det A \cdot \det B$(定理 3): 令 $2n \times 2n$ 阶辅助矩阵 $C = \begin{pmatrix} E & B \\ -A & 0 \end{pmatrix}$ 运用 II 型初等行变换将 C 化成

$$C' = \begin{pmatrix} E & B \\ 0 & AB \end{pmatrix}.$$

提示: 利用等式 $\det C = \det C'$ 和公式 (4),(5).

同样地, 证明也可以根据第 2 章 §3 习题 17,18 给出, 注意到 $\begin{pmatrix} E & A \\ 0 & E \end{pmatrix}$ 是上三角矩阵.

4. (扎哈洛夫 В. И. —— 图拉, 1984) 在平稳随机过程模型的研究中, 出现了下述行列式:

$$\Delta_n(k_1, x_1; \cdots; k_m, x_m) = \begin{vmatrix} M_{k_1}^n(x_1) \\ M_{k_2}^n(x_2) \\ \cdots\cdots \\ M_{k_m}^n(x_m) \end{vmatrix},$$

其中 $x_1, x_2, \cdots, x_m$ 是未知量; $k_1, \cdots, k_m$ 是自然数, $k_1 + k_2 + \cdots + k_m = n$; $M_k^n(x)$ 是 $k \times n$ 阶矩阵, 形如

$$M_k^n(x) = \begin{pmatrix} 1 & x & x^2 & \cdots & x^{n-1} \\ 0 & 1 & \binom{2}{1} x & \cdots & \binom{n-1}{1} x^{n-2} \\ 0 & 0 & 1 & \cdots & \binom{n-1}{2} x^{n-3} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \cdots & \binom{n-1}{k-1} x^{n-k} \end{pmatrix}.$$

证明

$$\Delta_n(k_1, x_1; \cdots; k_m, x_m) = \prod_{1 \leqslant j < i \leqslant m} (x_i - x_j)^{k_i k_j}.$$

提示: 当 $k_1 = \cdots = k_m = 1$ 时, 即当 $m = n$ 时, 得到范德蒙德行列式.

5. 证明

$$B_n(s,t)=\begin{vmatrix}\binom{s}{t} & \binom{s}{t+1} & \cdots & \binom{s}{t+n-1}\\ \binom{s+1}{t} & \binom{s+1}{t+1} & \cdots & \binom{s+1}{t+n-1}\\ \cdots & \cdots & \cdots & \cdots\\ \binom{s+n-1}{t} & \binom{s+n-1}{t+1} & \cdots & \binom{s+n-1}{t+n-1}\end{vmatrix}$$

$$=\frac{\binom{n+s-1}{n}\binom{n+s-2}{n}\cdots\binom{n+s-t}{n}}{\binom{n+t-1}{n}\binom{n+t-2}{n}\cdots\binom{n}{n}}.$$

提示：逐次从第 k 行中提出 $(s+k-1), k=1,2,\cdots,n$, 然后从第 l 列中提出 $\frac{1}{(t+l-1)}, l=1,2,\cdots,n$. 直到第一列中除了 1 之外不再含有其他元素.

6. 设

$$C_n(\lambda_1,\cdots,\lambda_n)=\begin{pmatrix}\lambda_1 & 1 & 0 & \cdots & 0 & 0 & 0\\ -1 & \lambda_2 & 1 & \cdots & 0 & 0 & 0\\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots\\ 0 & 0 & 0 & \cdots & \lambda_{n-2} & 1 & 0\\ 0 & 0 & 0 & \cdots & -1 & \lambda_{n-1} & 1\\ 0 & 0 & 0 & \cdots & 0 & -1 & \lambda_n\end{pmatrix}.$$

证明 $\det C_n=\lambda_n\det C_{n-1}+\det C_{n-2}$. 当 $\lambda_1=\lambda_2=\cdots=\lambda_n=1$ 时，求出数值 $\det C_n$.

提示：用第 2 章 §3 第 3 段的例 3, 并注意到事实 $\det C_n(1,\cdots,1)=(-1)^n\det C_n(-1,\cdots,-1)$.

7. 证明 $n\times n$ 矩阵

$$A_n=\begin{pmatrix}2 & -1 & 0 & 0 & \cdots & 0 & 0 & 0\\ -1 & 2 & -1 & 0 & \cdots & 0 & 0 & 0\\ 0 & -1 & 2 & -1 & \cdots & 0 & 0 & 0\\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots\\ 0 & 0 & 0 & 0 & \cdots & -1 & 2 & -1\\ 0 & 0 & 0 & 0 & \cdots & 0 & -1 & 2\end{pmatrix}$$

的行列式等于 $n+1$.

8. 设 A, B 是任意 n 阶方阵. 证明

$$\det\begin{pmatrix}A & B\\ B & A\end{pmatrix}=\det(A+B)\cdot\det(A-B).$$

9. 设 X 是 $n \times k$ 矩阵而 Y 是 $k \times n$ 矩阵. 证明

$$\det(E_n + XY) = \det(E_k + YX).$$

提示： 利用关系式

$$\begin{pmatrix} E_k + YX & 0 \\ X & E_n \end{pmatrix} \begin{pmatrix} E_k & Y \\ 0 & E_n \end{pmatrix} = \begin{pmatrix} E_k & Y \\ 0 & E_n \end{pmatrix} \begin{pmatrix} E_k & 0 \\ X & E_n + XY \end{pmatrix}.$$

§3 行列式的应用

1. 非退化矩阵的判别准则 根据第 2 章 §3 定理 5, 矩阵 $A \in M_n(\mathbb{R})$ 的非退化性 (即 $\operatorname{rank} A = n$) 等价于它的可逆性. 将 §2 定理 3 应用于关系式 $AA^{-1} = A^{-1}A = E$, 得到

$$\det A \cdot \det(A^{-1}) = 1.$$

因而, 非退化矩阵的行列式不等于零, 且

$$\det(A^{-1}) = (\det A)^{-1}.$$

给出矩阵 A, 我们可以同时考察它的 **伴随矩阵**

$$A^{\vee} = \begin{pmatrix} A_{11} & \cdots & A_{n1} \\ \cdots & \cdots & \cdots \\ A_{1n} & \cdots & A_{nn} \end{pmatrix}.$$

为了得到 $A^{\vee}$, 我们需要在矩阵 A 的每一个元素 a_{ij} 的位置放上它的代数余子式 $A_{ij}(i, j = 1, \cdots, n)$, 然后取转置.

定理 1 矩阵 $A \in M_n(\mathbb{R})$ 是非退化的 (可逆的), 当且仅当 $\det A \neq 0$. 若 $\det A \neq 0$, 则

$$A^{-1} = (\det A)^{-1} A^{\vee},$$

或更详细地写成

$$\begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \cdots & \cdots & \cdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix}^{-1} = \begin{pmatrix} \dfrac{A_{11}}{\det A} & \cdots & \dfrac{A_{n1}}{\det A} \\ \cdots & \cdots & \cdots \\ \dfrac{A_{n1}}{\det A} & \cdots & \dfrac{A_{nn}}{\det A} \end{pmatrix}.$$

在证明定理之前, 我们需要一个引理.

引理 设 $A \in M_n(\mathbb{R})$. 则有关系式

$$a_{i1}A_{j1} + a_{i2}A_{j2} + \cdots + a_{in}A_{jn} = \delta_{ij} \det A, \tag{1}$$

$$a_{1i}A_{1j} + a_{2i}A_{2j} + \cdots + a_{ni}A_{nj} = \delta_{ij} \det A, \tag{2}$$

其中 δ_{ij} 是克罗内克符号(当 $i \neq j$ 时，(1)(或 (2)) 叫作行列式 $\det A$ 按照错行 (或错列) 展开).

证明　当 $i = j$ 时，引理的结论与 §2 定理 1 一致. 因而只需考察 $i \neq j, \delta_{ij} = 0$ 的情况. 为此引入矩阵

$$A' = [A_{(1)}, \cdots, A_{(i)}, \cdots, A_{(i)}, \cdots, A_{(n)}] = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{i1} & a_{i2} & \cdots & a_{in} \\ \cdots & \cdots & \cdots & \cdots \\ a_{i1} & a_{i2} & \cdots & a_{in} \\ \cdots & \cdots & \cdots & \cdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix},$$

它是将矩阵 $A = [\cdots, A_{(i)}, \cdots, A_{(j)}, \cdots]$ 的第 j 行换成第 i 行得到的 (第 i 行保留不动). 如同所有带有两个相同行的方阵，$\det A' = 0$. 另一方面，代数余子式 $A'_{jk}(k = 1, \cdots, n)$, 是用划去 A' 的第 j 行 $A'_{(j)} = A_{(i)}$ 和第 k 列得到的，因此 $A'_{jk} = A_{jk}$. 将行列式 $A' = (a'_{st})$ 按照第 j 行展开，得到关系式

$$0 = \det A' = \sum_{k=1}^{n} a'_{jk} A'_{jk} = \sum_{k=1}^{n} a_{ik} A_{jk},$$

恰为引理中的 (1) 式. (2) 式可由关于列的类似性质得到. □

转入定理的证明，我们只要注意到 (1) 式的左边是矩阵 $C = AA^{\vee}$ 的元素 c_{ij}:

$$\begin{pmatrix} c_{11} & \cdots & c_{1n} \\ \cdots & \cdots & \cdots \\ c_{n1} & \cdots & c_{nn} \end{pmatrix} = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \cdots & \cdots & \cdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix} \begin{pmatrix} A_{11} & \cdots & A_{n1} \\ \cdots & \cdots & \cdots \\ A_{1n} & \cdots & A_{nn} \end{pmatrix}.$$

根据 (1) 式，$(c_{ij}) = (\delta_{ij} \det A) = (\det A)E$. 于是

$$AA^{\vee} = (\det A)E,$$

当 $\det A \neq 0$ 时，我们得到

$$(\det A)^{-1}(AA^{\vee}) = A(\det A)^{-1}A^{\vee} = E.$$

(2) 式的左边是矩阵 $C' = A^{\vee}A$ 的元素 c'_{ij} 的表达式. 因为 (1) 和 (2) 的右边是相同的，故当 $\det A \neq 0$ 时，我们得到

$$A(\det A)^{-1}A^{\vee} = (\det A)^{-1}A^{\vee}A = E,$$

于是 $A^{-1} = (\det A)^{-1} A^{\vee}$. □

推论 一个行列式等于零，当且仅当它的行 (或列) 线性相关.

证明 矩阵 $A \in M_n(\mathbb{R})$ 的行 (或列) 的线性相关性，等价于 $\text{rank}A < n$, 即矩阵 A 的退化性，根据定理 1, 等价于条件 $\det A = 0$. □

注记 $\text{rank}A < n \Rightarrow \det A = 0$ 实际上是行列式基本性质的直接推论 (见 §2,D2,D6).

定理 1 的理论价值 (比实用价值) 大. 从计算的角度来看，特别是当矩阵的阶数较大时，求逆矩阵 A^{-1} 用第 2 章 §7 给出的 (P, Q) 算法更方便一些.

2. 克拉默公式 现在我们来推导含 n 个未知数， n 个方程的线性方程组的求解公式，行列式理论最初的发展就是为了这件事情.

定理 2(克拉默) 如果线性方程组

$$\begin{gathered} a_{11}x_1 + \cdots + a_{1n}x_n = b_1, \\ \cdots\cdots\cdots\cdots \\ a_{n1}x_1 + \cdots + a_{nn}x_n = b_n \end{gathered}$$

的系数行列式非零 (即 $\det(a_{ij}) \neq 0$), 则它有下述唯一解:

$$x_k^0 = \frac{\begin{vmatrix} a_{11} & \cdots & b_1 & \cdots & a_{1n} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ a_{n1} & \cdots & b_n & \cdots & a_{nn} \end{vmatrix}}{\begin{vmatrix} a_{11} & \cdots & a_{1k} & \cdots & a_{1n} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ a_{n1} & \cdots & a_{nk} & \cdots & a_{nn} \end{vmatrix}}, \qquad k = 1, 2, \cdots, n$$

(其中分子 D_k 是用自由项组成的列替换 $D = \det(a_{ij})$ 中的第 k 列得到的).

证明 根据定理 1, 矩阵 $A = (a_{ij})$ 可逆. 因此将我们的方程组写成 $AX = B$ 的形式，如同第 2 章 §3 第 8 段那样，我们得到

$$\begin{pmatrix} x_1^0 \\ \vdots \\ x_k^0 \\ \vdots \\ x_n^0 \end{pmatrix} = A^{-1}B = \frac{1}{\det A} \begin{pmatrix} A_{11} & A_{21} & \cdots & A_{n1} \\ A_{12} & A_{22} & \cdots & A_{n2} \\ \cdots & \cdots & \cdots & \cdots \\ A_{1n} & A_{2n} & \cdots & A_{nn} \end{pmatrix} \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix},$$

从而

$$x_k^0 = \frac{1}{\det A} \sum_{i=1}^{n} A_{ik} b_i = \frac{1}{\det A}(b_1 A_{1k} + b_2 A_{2k} + \cdots + b_n A_{nk}), k = 1, 2, \cdots, n.$$

其中分子的表达式恰为行列式 D_k 按照第 k 列的展开式 (见公式 (2)).

将上述的全部过程反推回去，可以看到 $\left(\frac{D_1}{\det A},\cdots,\frac{D_n}{\det A}\right)$ 确实是方程组的解. □

注意到第 1 章 §4 的公式 (3) 、 (9) 分别与 $n=2$ 和 $n=3$ 时的克拉默公式一致. 当 n 较小时，用克拉默公式 (解线性方程组) 是方便的，在一般情况下，可以把克拉默公式看作纯理论函数. 例如将其用于在第 1 章 §3 第 5 段中给出的线性方程组，就得到斐波那契数的表达式 (考虑到 $\det A=1$)

$$f_n=\begin{vmatrix} 1 & 0 & 0 & \cdots & 0 & 0 & 1 \\ 0 & 1 & 0 & \cdots & 0 & 0 & 1 \\ -1 & -1 & 1 & \cdots & 0 & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \cdots & -1 & 1 & 0 \\ 0 & 0 & 0 & \cdots & -1 & -1 & 0 \end{vmatrix}.$$

显然它比我们在第 2 章 §3 第 5 段中求出的关于 f_n 的清晰的表达式相差甚远.

还应当指出，使用克拉默公式的不可或缺的条件 $\det A\neq 0$ 有时是不稳定的. 对于实用中带有近似系数的线性方程组，计算精确度的提高可能会使情况发生根本的改变. 例如

$$A_\varepsilon=\begin{pmatrix} -1 & 10 & 0 & \cdots & 0 & 0 \\ 0 & -1 & 10 & \cdots & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \cdots & -1 & 10 \\ \varepsilon & 0 & 0 & \cdots & 0 & -1 \end{pmatrix}\in M_{10}(\mathbb{R}),$$

则 $\det A_\varepsilon=1-\varepsilon\cdot 10^9$(将行列式按照第一列的元素展开). 当 $\varepsilon=10^{-9}$ 时, 有 $\det A_\varepsilon=0$. 同时，若系数矩阵的计算仅仅精确到百万分之一，我们可以“忽略 ε”(即令 $\varepsilon=0$, 则 $\det A=1$). 由此看来，克拉默公式的适用条件对系数系统的微小“扰动”是敏感的.

3. 加边子式法 第 2 章 §3 包含了求长方形线性方程组解集的全部所需资料. 在这一过程中, 矩阵的秩的概念至关重要. 我们仅需将其转化为行列式理论的语言，就可以得到计算矩阵秩的另一种方法以及判断线性空间 $\mathbb{R}^m$ 中的向量组线性无关性的便利手段.

设

$$A=\begin{pmatrix} a_{11} & \cdots & a_{1r} & \cdots & a_{1n} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ a_{r1} & \cdots & a_{rr} & \cdots & a_{rn} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ a_{m1} & \cdots & a_{mr} & \cdots & a_{mn} \end{pmatrix}$$

是任意一个 $m \times n$ 阶长方矩阵，其系数 $a_{ij} \in \mathbb{R}$.

定义 $m \times n$ 矩阵 A 的任意 k 行和 k 列 $(k \leqslant \min(m,n))$ 交叉处的元素组成一个方阵，其行列式叫作 A 的一个 k**阶子式**. 如果 $i_1, \cdots, i_k$ 和 $j_1, \cdots, j_k$ 分别是行指标和列指标，子式记作

$$M\begin{pmatrix} i_1 & \cdots & i_k \\ j_1 & \cdots & j_k \end{pmatrix}.$$

当 $m = n$ 且 $k = n-1$ 时，我们就得到了先前引入的 $n \times n$ 矩阵 A 的子式 M_{ij}.

子式 $\widetilde{M}$ 叫作 M 的 **加边**, 若 M 是由 $\widetilde{M}$ 去掉一端的行 (第一行或最后一行), 以及一端的列得到的.

定理(加边子式法) 在计算矩阵 A 的秩时，可由 A 中较小阶的子式转到较大阶的子式. 如果已找到 A 的一个 r 阶子式 $M \neq 0$, 那么仅需计算 $r+1$ 阶子式，即子式 M 的加边. 如果它们都等于零，则 $\operatorname{rank} A = r$.

证明 论断基于一个简单的事实，如果矩阵 A 的全部 k 阶子式等于零，则任意更高阶的子式亦等于零. 为此，根据 §2 定理 1, 观察任意 $(k+1)$ 阶子式按照任意列的元素的展开式 (例如第一或最后一列，如果仅限于考察借助加边得到的子式), 然后进入 $(k+2)$ 阶子式，等等.

按照定理叙述中所指出的模式，设我们已达到某个 r 阶子式 $M \neq 0$. 不失一般性，假设与 M 相应的矩阵位于矩阵 A 的左上角：

$$A = \left|\begin{array}{ccc|ccccc} a_{11} & \cdots & a_{1r} & \cdots & a_{1j} & \cdots & a_{1n} \\ & M & & & \cdots\cdots & & \\ a_{r1} & \cdots & a_{rr} & \cdots & a_{rj} & \cdots & a_{rn} \\ \hline \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ a_{i1} & \cdots & a_{ir} & \cdots & a_{ij} & \cdots & a_{in} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ a_{m1} & \cdots & a_{mr} & \cdots & a_{mj} & \cdots & a_{mn} \end{array}\right|.$$

这件事总可以通过交换矩阵的行与列做到，自然地，这种作法不改变矩阵 A 的秩.

现在在 A 中取出任意一行 $A_{(i)}$ 和任意一列 $A^{(j)}$(可能 $i \leqslant r$ 或 $j \leqslant r$). 在 $A_{(i)}$ 和 $A^{(j)}$ 的元素的帮助下我们组成了一个 $r+1$ 阶子式 $\widetilde{M}$, 它是 M 的加边：

$$\widetilde{M} = \begin{vmatrix} a_{11} & \cdots & a_{1r} & a_{1j} \\ \cdots & \cdots & \cdots & \cdots \\ a_{r1} & \cdots & a_{rr} & a_{rj} \\ a_{i1} & \cdots & a_{ir} & a_{ij} \end{vmatrix}.$$

如果 $\widetilde{M} \neq 0$, 我们再来考虑 $\widetilde{M}$ 的加边. 当 M 的全部加边子式为零时，我们就到达了临界时刻.

设对于任意 $i, j, \widetilde{M} = 0$. 将 $\widetilde{M}$ 按照最后一行展开，得到关系式

$$a_{i1}M_1 + a_{i2}M_2 + \cdots + a_{ir}M_r + a_{ij}M = 0,$$

其中系数

$$M_s = (-1)^{r+s+1} \begin{vmatrix} a_{11} & \cdots & a_{1,s-1} & a_{1,s+1} & \cdots & a_{1r} & a_{1j} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ a_{r1} & \cdots & a_{r,s-1} & a_{r,s+1} & \cdots & a_{rr} & a_{rj} \end{vmatrix},$$

不依赖于 i 的选择. 因为 $M \neq 0$, 故

$$a_{ij} = \lambda_1 a_{i1} + \lambda_2 a_{i2} + \cdots + \lambda_r a_{ir},$$

其中 $\lambda_s = \dfrac{-M_s}{M}, 1 \leqslant s \leqslant r$, 此式对 $i = 1, 2, \cdots, m$ 均成立. 于是

$$A^{(j)} = \lambda_1 A^{(1)} + \lambda_2 A^{(2)} + \cdots + \lambda_r A^{(r)},$$

即矩阵 A 的任意一列是前 r 列的线性组合. 这就表明 $\text{rank}\, A \leqslant r$. 但是从 $M \neq 0$, 得到 M 中的列是线性无关的，自然地，它们所对应的 A 当中更长的列也是线性无关的. 我们得到了结论 $\text{rank}\, A = r$. □

推论　任意矩阵的秩等于它的非零子式的最大阶数.

推论亦可独立于定理进行证明. 设矩阵 A 的秩等于 r. 根据第 2 章 §2 定理 1, r 是矩阵 A 的线性无关行的最大个数，也是线性无关列的最大个数. 运用第 2 章 §3 定理 6, 我们发现

$$A = B \begin{pmatrix} E_r & 0 \\ 0 & 0 \end{pmatrix} C,$$

其中 B 和 C 分别是非退化的 m 阶和 n 阶方阵，可以写成初等矩阵的乘积. 因为矩阵 $\begin{pmatrix} E_r & 0 \\ 0 & 0 \end{pmatrix}$ 有一个非零 r 阶子式 $M = |E_r| = 1$, 但是没有阶数 $> r$ 的非零子式，又因为这一性质在行与列的初等变换下保持不变，我们就得到了所需的论断. □

加边子式法是相当实用的，特别是当我们不仅想知道秩，也想知道矩阵 A 的行或列的极大线性无关组的时候. 然而在初等变换下这一信息是会失掉的.

习　题

1. 证明下述公式：

$$(AB)^\vee = B^\vee A^\vee; \quad ({}^tA)^\vee = {}^t(A^\vee);$$

$$(\lambda A)^\vee = \lambda^{n-1} A^\vee; \quad (A^\vee)^\vee = (\det\, A)^{n-2} A.$$

2. 通过 $\text{rank}\, A$ 表示 $\text{rank}\, A^\vee$.

3. 证明当未知量的个数与方程的个数相等时，齐次线性方程组有非零解，当且仅当系数矩阵的行列式等于零.

4. 运用第 2 章 §3 第 8 段的结果和定理 2 证明，当秩 $r=n-1$ 时，齐次线性方程组

$$\begin{gathered} a_{11}x_1+\cdots+a_{1n}x_n=0, \\ \cdots\cdots\cdots\cdots \\ a_{n-1,1}x_1+\cdots+a_{n-1,n}x_n=0 \end{gathered}$$

的基础解系由一个列向量

$$X^0=[D_1,-D_2,D_3,\cdots,(-1)^{n-1}D_n]$$

组成，其中 D_i 是从 $A=(a_{ij})$ 中去掉第 i 列所得矩阵的行列式. 任意解的形式为 $X=\lambda X^0$.

5. 设 $A=(a_{ij})\in M_n(\mathbb{R})$, 且任取 $i\neq j$, 有 $(n-1)|a_{ij}|<|a_{ii}|$. 证明 $\det A\neq 0$.

提示： 假设命题不真，利用习题 3 给出的准则. 即如果 $[x_1^0,\cdots,x_n^0]$ 是线性方程组 $AX=0$ 的非平凡解，且 x_k^0 是它的具有极大模的分量，则从第 k 个方程

$$a_{kk}x_k^0+\sum_{j\neq k}a_{kj}x_j^0=0$$

得到的估值

$$(n-1)|a_{kk}||x_k^0|=(n-1)\left|\sum_{j\neq k}a_{kj}x_j^0\right|<(n-1)|a_{kk}||x_k^0|,$$

得到矛盾.

6. 证明下述论断 (比内 – 柯西定理)　设 $A=(a_{ij}),B=(b_{kl})$ 分别是 $n\times m$ 和 $m\times n$ 阶矩阵，且 $C=AB$. 则

$$\det C=\sum_{1\leqslant j_1\leqslant\cdots\leqslant j_n\leqslant m}\begin{vmatrix} a_{1j_1} & a_{2j_1} & \cdots & a_{nj_1} \\ a_{1j_2} & a_{2j_2} & \cdots & a_{nj_2} \\ \cdots & \cdots & \cdots & \cdots \\ a_{1j_n} & a_{2j_n} & \cdots & a_{nj_n}\end{vmatrix}\times\begin{vmatrix} b_{j_11} & b_{j_12} & \cdots & b_{j_1n} \\ b_{j_21} & b_{j_22} & \cdots & b_{j_2n} \\ \cdots & \cdots & \cdots & \cdots \\ b_{j_n1} & b_{j_n2} & \cdots & b_{j_nn}\end{vmatrix}.$$

右边的和式遍历从 $1,2,\cdots,m$ 中取 n 个元素 $\{j_1,j_2,\cdots,j_n\}$ 的所有可能的 $\begin{pmatrix} m \\ n\end{pmatrix}$ 种组合. 特别地，当 $m=n$ 时， $\det C=\det A\cdot\det B$, 而当 $n>m$ 时， $\det C=0$.

提示： 因为

$$C=(c_{ij}),\quad c_{ij}=\sum_{k=1}^m a_{ik}b_{kj},$$

反复运用行列式的性质 D2(§1 定理 2) 得到

$$\det C=\sum_{k_1,\cdots,k_n=1}^m\begin{vmatrix} a_{1k_1} & a_{1k_2} & \cdots & a_{1k_n} \\ a_{2k_1} & a_{2k_2} & \cdots & a_{2k_n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{nk_1} & a_{nk_2} & \cdots & a_{nk_n}\end{vmatrix}b_{k_11}b_{k_22}\cdots b_{k_nn},$$

其中求和遍历所有两两不同的 $k_1,\cdots,k_n$. 当 $m<n$ 时，没有这样的下标，故 $\det C=0$. 如果 $m\geqslant n$, 则 $k_1,\cdots,k_n$ 就是从 $1,2,\cdots,m$ 所取的元素 $\{j_1,\cdots,j_n\}$ 按某种顺序的排列，将对应于给定组合 $\{j_1,\cdots,j_n\}$ 的所有的项收集到一起，并在 §1 公式 (3) 的帮助下就可以得到所需的表达式：

$$\sum\begin{vmatrix} a_{1k_1} & \cdots & a_{nk_1} \\ \multicolumn{3}{c}{\cdots\cdots\cdots\cdots\cdots} \\ a_{1k_n} & \cdots & a_{nk_n}\end{vmatrix} b_{k_1 1}\cdots b_{k_n n}=\begin{vmatrix} a_{1j_1} & \cdots & a_{nj_1} \\ \multicolumn{3}{c}{\cdots\cdots\cdots\cdots\cdots} \\ a_{1j_n} & \cdots & a_{nj_n}\end{vmatrix}\sum \varepsilon_\pi b_{k_1 1}\cdots b_{k_n n}$$

$$=\begin{vmatrix} a_{1j_1} & \cdots & a_{nj_n} \\ \multicolumn{3}{c}{\cdots\cdots\cdots\cdots\cdots} \\ a_{nj_1} & \cdots & a_{nj_n}\end{vmatrix}\cdot\begin{vmatrix} b_{j_1 1} & \cdots & b_{j_1 n} \\ \multicolumn{3}{c}{\cdots\cdots\cdots\cdots\cdots} \\ b_{j_n 1} & \cdots & b_{j_n n}\end{vmatrix},$$

其中 $\pi=\begin{pmatrix} j_1 & \cdots & j_n \\ k_1 & \cdots & k_n\end{pmatrix}$.

7. 利用上题证明，如果 A 是 $\mathbb{R}$ 上的 $m\times n$ 矩阵，$m\geqslant n$, 则

$$\det {}^tAA=\sum_M M^2,$$

其中 M 遍历矩阵 A 的全部 $\begin{pmatrix} m \\ n\end{pmatrix}$ 个 n 阶子式.

8. 给定 $n\times n$ 矩阵 $A=(a_{ij})$ 的一个 k 阶子式 (见第 3 段的定义)

$$M\begin{pmatrix} i_1 & \cdots & i_k \\ j_1 & \cdots & j_k\end{pmatrix}$$

相应的 $(n-k)$ 阶余子式 $\overline{M}\begin{pmatrix} i_1 & \cdots & i_k \\ j_1 & \cdots & j_k\end{pmatrix}$ 是从 A 中去掉第 $i_1,\cdots,i_k$ 行，和第 $j_1,\cdots,j_k$ 列所得矩阵的行列式. 表达式

$$A\begin{pmatrix} i_1 & \cdots & i_k \\ j_1 & \cdots & j_k\end{pmatrix}=(-1)^{s(M)}\overline{M}\begin{pmatrix} i_1 & \cdots & i_k \\ j_1 & \cdots & j_k\end{pmatrix},$$
$$s(M)=(i_1+\cdots+i_k)+(j_1+\cdots+j_k),$$

称为 $M\begin{pmatrix} i_1 & \cdots & i_k \\ j_1 & \cdots & j_k\end{pmatrix}$ 的**代数余子式**. 当 $k=n-1$ 时，我们回到通常代数余子式的定义. 利用行列式按照第 $i_1,\cdots,i_k$ 行元素的一系列展开证明下述

定理(拉普拉斯) 在矩阵 $A=(a_{ij})$ 中取下标为 $i_1,\cdots,i_k$ 的 k 行. 则

$$\det A=\sum_{1\leqslant j_1<\cdots<j_k\leqslant n} M\begin{pmatrix} i_1 & \cdots & i_k \\ j_1 & \cdots & j_k\end{pmatrix}\cdot A\begin{pmatrix} i_1 & \cdots & i_k \\ j_1 & \cdots & j_k\end{pmatrix}.$$

任取正整数 n, 在两种特殊情况下，拉普拉斯定理是我们已知的： 1)$k=1$; 2)A 有阶数为 $(n-k)\times k$ 的一个零角. 在未知的情况下，哪怕取 $n=4, i_1=1, i_2=2$ 对拉普拉斯定理的正确

性作一说明也是有益的：

$$\det A=\begin{vmatrix}a_{11}&a_{12}\\a_{21}&a_{22}\end{vmatrix}\cdot\begin{vmatrix}a_{33}&a_{34}\\a_{43}&a_{44}\end{vmatrix}-\begin{vmatrix}a_{11}&a_{13}\\a_{21}&a_{23}\end{vmatrix}\cdot\begin{vmatrix}a_{32}&a_{34}\\a_{42}&a_{44}\end{vmatrix}$$
$$+\begin{vmatrix}a_{11}&a_{14}\\a_{21}&a_{24}\end{vmatrix}\cdot\begin{vmatrix}a_{32}&a_{33}\\a_{42}&a_{43}\end{vmatrix}+\begin{vmatrix}a_{12}&a_{13}\\a_{22}&a_{23}\end{vmatrix}\cdot\begin{vmatrix}a_{31}&a_{34}\\a_{41}&a_{44}\end{vmatrix}$$
$$-\begin{vmatrix}a_{12}&a_{14}\\a_{22}&a_{24}\end{vmatrix}\cdot\begin{vmatrix}a_{31}&a_{33}\\a_{41}&a_{43}\end{vmatrix}+\begin{vmatrix}a_{13}&a_{14}\\a_{23}&a_{24}\end{vmatrix}\cdot\begin{vmatrix}a_{31}&a_{32}\\a_{41}&a_{42}\end{vmatrix}.$$

9. 设 $A\in M_n(\mathbb{R}), B\in M_m(\mathbb{R})$ 是非退化矩阵，C 是任意 $n\times m$ 矩阵. 利用矩阵的分块乘法 (见第 2 章 §3 习题 17) 证明

$$\begin{pmatrix}A&C\\0&B\end{pmatrix}^{-1}=\begin{pmatrix}A^{-1}&-A^{-1}CB^{-1}\\0&B^{-1}\end{pmatrix}.$$

10. 证明：若 $A,B,C,D\in M_n(\mathbb{R}),\det\ A\neq 0$ 则

$$\det\begin{pmatrix}A&B\\C&D\end{pmatrix}=\det(AD-ACA^{-1}B)$$
$$=(\det A)\cdot\det(D-CA^{-1}B).$$

此外，验证

$$\det\begin{pmatrix}A&B\\C&D\end{pmatrix}=\begin{cases}\det(AD-CB), & 若AC=CA,\\ \det(DA-CB), & 若AB=BA.\end{cases}$$

§4 行列式的公理化构造

§1 的定理 2 和定理 3 本质上给出了函数 det 的公理化描述，尽管我们纯粹从行列式的结构问题入手. 我们在本节中再指出通往行列式理论的若干途径，但每次仅局限于勾勒论证要点 (把它们补充完全将是很好的练习).

1. 第一公理化构造 将行列式看作满足下述三条性质的任意函数 $\mathcal{D}: M_n(\mathbb{R})\to\mathbb{R}$:

1.1) $\mathcal{D}(A)$ 关于矩阵 A 的行是斜对称的；

1.2) $\mathcal{D}(A)$ 关于矩阵 A 的行是多重线性的；

1.3) $\mathcal{D}(E)=1$.

我们看到，函数 $\mathcal{D}$ 是由性质 1.1)—1.3) 唯一确定的，并且符合 §1 中由完全展开式 (3) 给出的函数 det. 唯一需要关心的是，给出公式 $\mathcal{D}({}^tA)=\mathcal{D}(A)$ 的独立证明. 如果愿意，§1 的公式 (3) 本身同样需要推导.

2. 第二公理化构造 将行列式看作满足下述三条性质的任意函数 $\mathcal{D}: M_n(\mathbb{R})\to\mathbb{R}$:

2.1) $\mathcal{D}(\cdots,\lambda A_{(i)},\cdots)=\lambda\mathcal{D}(\cdots,A_{(i)},\cdots)$, 即如果矩阵 A 的某行 $A_{(i)}$ 乘以 λ, 则其行列式为 $\mathcal{D}(A)$ 乘以 λ;

2.2) $\mathcal{D}(\cdots,A_{(i)},\cdots,A_{(j)},\cdots)=\mathcal{D}(\cdots,A_{(i)}+A_{(j)},\cdots,A_{(j)},\cdots)$;

2.3) $\mathcal{D}(E)=1$.

依次验证:

a) 数值 $\mathcal{D}(A)$ 在矩阵 A 的 (Ⅱ) 型初等行变换下不变;

b) $\mathcal{D}(A)$ 是关于矩阵 A 的行的多重线性函数;

c) 当矩阵 A 有两行相等时, $\mathcal{D}(A)=0$, 从而 $\mathcal{D}(A)$ 是关于行的斜对称函数.

我们显然回到了第一公理化构造. 正规化性质 $\mathcal{D}(E)=1$ 在两种情况下都是不可或缺的.

3. 完全归纳构造法　将 1 阶矩阵 (a_{11}) 的行列式定义为 a_{11}. 2 阶和 3 阶矩阵的行列式分别由第 1 章 §4 的公式 (2) 和公式 (8) 定义. 设阶数为 $1,2,\cdots,n-1$ 的矩阵的行列式已定义. n 阶矩阵 $A=(a_{ij})$ 的行列式定义为

$$\mathcal{D}(A)=a_{11}M_{11}-a_{21}M_{21}+\cdots+(-1)^{n-1}a_{n1}M_{n1},$$

其中 M_{ij} 是矩阵 A 中对应于元素 a_{ij} 的 "子式", 它是 $(n-1)$ 阶矩阵 $\overline{A}$ 的行列式 $\mathcal{D}(\overline{A})$, 而 $\overline{A}$ 是去掉矩阵 A 的第 i 行和第 j 列得到的. 这样, 我们的定义性质实质上取了行列式按照第 1 列元素的展开式 (§2 定理 1 的特殊情况).

我们需要对 n 作归纳, 确立函数 $\mathcal{D}$ 的性质 1.1)—1.3) 对于 n 阶矩阵成立, 不要忘记这些性质对于 $(n-1)$ 阶行列式 M_{ij} 是成立的. 本段可归结为正确运用数学归纳法的技能, 它的实现不很复杂. 细节可参见教科书《代数学引论》 (1977 年).

4. 通过乘法性质的刻画　设我们有满足下述性质的函数 $\mathcal{D}: M_n(\mathbb{R})\to\mathbb{R}$

i) 任取矩阵 $A,B\in M_n(\mathbb{R}),\mathcal{D}(AB)=\mathcal{D}(A)\cdot\mathcal{D}(B)$;

ii) 任取初等矩阵 $F_{s,t}$(见第 2 章 §3 第 6 段),$\mathcal{D}(F_{s,t})=-1$;

iii) 任取形如

$$A=\begin{pmatrix}\lambda & & & *\\ & 1 & & \\ & & \ddots & \\ & & & 1\end{pmatrix},\quad \lambda\in\mathbb{R}$$

的上三角矩阵, $\mathcal{D}(A)=\lambda$. 特别地, $\mathcal{D}(F_1(\lambda))=\lambda$.

可以断言, $\mathcal{D}=\det$. 事实上, 将性质 i) 和 ii) 应用于初等矩阵

$$F_s(\lambda)=F_{1,s}\cdot F_1(\lambda)\cdot F_{1,s},$$

我们得到

$$\mathcal{D}(F_s(\lambda))=(-1)\cdot\lambda\cdot(-1)=\lambda,$$

并且根据矩阵 $F_s(\lambda)$ 的定义，此式对任意 $\lambda \in \mathbb{R}$ 成立，不仅对 $\lambda \neq 0$. 进而从

$$\begin{pmatrix} E_r & 0 \\ 0 & 0 \end{pmatrix} = F_{r+1}(0) \cdots F_n(0),$$

我们有

$$\mathcal{D}\begin{pmatrix} E_r & 0 \\ 0 & 0 \end{pmatrix} = \begin{cases} 0, & 若 r < n, \\ 1, & 若 r = n. \end{cases}$$

根据 iii), 对任意初等矩阵 $F_{s,t}(\lambda)$,$s < t$,$\mathcal{D}(F_{s,t}(\lambda)) = 1$. 因为

$$F_{s,t}F_{s,t}(\lambda)\ F_{s,t} = F_{t,s}(\lambda)$$

故 $\mathcal{D}(F_{t,s}(\lambda)) = 1$, 因此任取下标 $s \neq t$,

$$\mathcal{D}(F_{s,t}(\lambda)) = 1.$$

于是,

$$\mathcal{D}(F_{s,t}) = -1 = \det\ F_{s,t}, \quad \mathcal{D}(F_{s,t}(\lambda)) = 1 = \det\ F_{s,t}(\lambda),$$
$$\mathcal{D}(F_s(\lambda)) = \lambda = \det\ F_s(\lambda).$$

因为任意矩阵 $A \in M_n(\mathbb{R})$ 可以写成

$$A = P\begin{pmatrix} E_r & 0 \\ 0 & 0 \end{pmatrix}Q, \qquad r \leqslant n,$$

的形式，其中 P 和 Q 是初等矩阵的乘积 (见第 2 章 §3 定理 6 前的论证), 性质 i) 使我们断定 $\mathcal{D}(A) = \det\ A$.

习　题

1. (布朗金，波兰). 设 $f : \mathbb{R} \to \mathbb{R}$ 是满足条件 $f(0) = 0$ 的任意函数. 证明存在满足下述性质的唯一函数 $\mathcal{D} : M_n(\mathbb{R}) \to \mathbb{R}$:

i) 如果 A 有一列为零，则 $\mathcal{D}(A) = 0$;

ii) 如果 A' 从 A 经 (Ⅱ) 型初等列变换得到，则 $\mathcal{D}(A') = \mathcal{D}(A)$;

iii) 如果 $A = \mathrm{diag}(\lambda, 1, 1, \cdots, 1)$ 是对角矩阵，则 $\mathcal{D}(A) = f(\lambda)$.

当 $f(\lambda) = \lambda$ 时，我们有 $\mathcal{D} = \det$, 但 f 取法的任意性在某些实际问题中是有用的.

2. 建议读者提出并论证各自不同的公理化方法来描述函数 det.

第 4 章　群. 环. 域

在前几章中我们积累了大量的具体材料，现在应该从更一般的观点对它们加以考察. 为此我们将在本章中引入并研究 (仍停留在初等水平上) 群. 环. 域的概念，它们在代数学的所有概念中是最基本的.

§1　具有代数运算的集合

1. 二元运算　设 X 是任意集合. 从笛卡儿平方 $X^2 = X \times X$ 到 X 的一个任意 (确定) 的映射 $\tau : X \times X \to X$ 叫作 X 上的 **二元代数运算**(或合成律). 这样，任取元素 $a, b \in X$, 有序对 (a, b) 对应于 X 中唯一确定的元素 $\tau(a, b)$. 有时将 $\tau(a, b)$ 写成 $a\tau b$, 并通常引入特殊的记号： $*, \circ, \cdot$ 或 $+$, 等等来表示 X 上的二元运算. 按照这种记法，我们以后称 $a \cdot b$(或简记作 ab, a 和 b 之间没有任何记号) 为 a 与 b 的 **积**, 而 $a + b$ 为 a 与 b 的 **和**, 显然这些名称在大多数情况下是约定的.

一般来说，在集合 X 上可以定义多种不同的运算. 从中选定一种后，比如使用记号： $(X, *)$, 则称运算 $*$ 定义了 X 上的一种 **代数结构**, 或 $(X, *)$ 是一个 **代数结构** (亦称 **代数系统**). 例如在整数集 $\mathbb{Z}$ 上，除了自然的 $+, \cdot$(加法和乘法) 外，很容易在 $+$(或 $-$) 和 $\cdot$ 的帮助下得到各种 "导出" 运算： $n \circ m = n + m - nm$, $n * m = -n - m$, 等等. 我们就有了不同的代数结构 $(\mathbb{Z}, +)$, $(\mathbb{Z}, \cdot)$, $(\mathbb{Z}, \circ)$, $(\mathbb{Z}, *)$.

除了二元运算之外，我们不过多地关注更一般的 n 元运算及其他们的组合 (如 $n = 1$ 时的一元运算， $n = 3$ 时的三元运算等等). 与之相应的代数结构组成了一个专门的理论，泛代数. 我们提到这一点，仅仅是为了再次强调带有二元运算的代数结构在数学中本质上的重要意义，这种结构看来是泛代数的特殊部分.

显然，在集合 X 上可以定义无限多种二元运算结构，然而研究任意代数结构的问题过于一般，难以得出具体的、有实际意义的结论. 因此我们仅限于研究几种自然的代数结构.

2. 半群和幺半群　定义在集合 X 上的二元运算 $*$ 称为 **结合的**, 若任取 a, b,

$c \in X$,

$$(a * b) * c = a * (b * c);$$

$*$ 称为 **交换的**, 若

$$a * b = b * a.$$

同样的称谓亦适用于相应的代数结构 $(X, *)$.

结合性和交换性是相互独立的. 例如在 $\mathbb{Z}$ 上定义的运算 $*$:

$$n * m = -n - m$$

显然是交换的，但是

$$(1 * 2) * 3 = (-1 - 2) * 3 = -(-1 - 2) - 3 = 0 \neq 4 = 1 * (2 * 3),$$

因而不是结合的. 另一方面，在阶数 $n > 1$ 的全体 n 阶方阵的集合 $M_n(\mathbb{R})$ 上定义的乘法运算是结合的，但不交换 (见第 2 章 §3 第 2 段).

元素 $e \in X$ 叫作关于 二元运算 $*$ 的 **单位元** (或 **中性元**), 若任取 $x \in X, e * x = x * e = x$. 如果 e' 也是一个单位元，则根据定义， $e' = e' * e = e$. 因而在一个代数结构 $(X, *)$ 中最多只有一个单位元.

集合 X 连同其上给定的满足结合律的二元运算称为一个 **半群**. 带有单位元的半群通常称为 **幺半群**(或 **有单位元的半群**).

与任意的集合一样，幺半群 $M = (M, *)$ 的基数记作 Card M 或 $|M|$. 如果 M 中只有有限多个元素，称 M 为 $|M|$ 阶有限幺半群. 我们来看半群和幺半群的一些例子.

例 1 设 Ω 是任意集合，且 $M(\Omega)$ 是它的变换的集合 (即 Ω 到自身的映射). 从集合与映射的性质可以推出 (第 1 章 §5),$M(\Omega)$ 是一个幺半群. 我们有三元组 $(M(\Omega), \circ, e_\Omega)$, 其中 $\circ$ 是映射的自然合成，而 e_Ω 是恒等映射.

我们区分出 Ω 是有限集的特殊情况, 若 $|\Omega| = n$, 将其元素简记作正整数 $1, 2, \cdots, n$. 每一个映射 $f : \Omega \to \Omega$ 可由一个有序数列 $f(1), f(2), \cdots, f(n)$ 确定，其中 $f(i)$ 可以取 Ω 的任意元素. 不排除当 $i \neq j$ 时， $f(i) = f(j)$. 取遍所有可能的序列，我们得到 n^n 个变换. 于是 $|M(\Omega)| = \text{Card } M(\Omega) = n^n$. 设 $n = 2$, 则幺半群 $M(\{1, 2\})$ 的元素 e, f, g, h 及其乘法由下述两个表完全确定:

	1	2
e	1	2
f	2	1
g	1	1
h	2	2

$\cdot$	e	f	g	h
e	e	f	g	h
f	f	e	h	g
g	g	g	g	g
h	h	h	h	h

显然， $M(\{1, 2\})$ 是一个非交换幺半群.

例 2 再次设 Ω 是任意集合，且 $\mathcal{P}(\Omega)$ 是它的子集的集合 (见第 1 章 §5 习题 4). 因为 $(A\cap B)\cap C=A\cap(B\cap C)$ 和 $(A\cup B)\cup C=A\cup(B\cup C)$, 故 $\mathcal{P}(\Omega)$ 上有两种自然的结合二元运算. 显然 $\varnothing\cup A=A, A\cap\Omega=A$. 我们得到两个可交换的幺半群: $(\mathcal{P}(\Omega),\cup,\varnothing)$ 和 $(\mathcal{P}(\Omega),\cap,\Omega)$, 如果 $|\Omega|=n$, 则 $|\mathcal{P}(\Omega)|=2^n$.

例 3 $(M_n(\mathbb{R}),+,0)$ 是以零矩阵为单位元的交换幺半群，而 $(M_n(\mathbb{R}),\cdot,E)$ 是以单位矩阵为单位元的非交换幺半群，这从我们熟知的第 2 章中矩阵的加法与乘法的性质可以直接推断出来.

例 4 设 n 是任意确定的正整数， $n\mathbb{Z}=\{nm|m\in\mathbb{Z}\}$ 是可以被 n 除尽的整数集. 则 $(n\mathbb{Z},+,0)$ 是交换幺半群，而 $(n\mathbb{Z},\cdot)$ 当 $n>1$ 时是没有单位元的半群.

例 5 n 阶随机矩阵的集合 $P_n(\mathbb{R})$(见第 2 章 §3 的习题 4) 关于通常矩阵的乘法构成一个幺半群.

带有运算 $*$ 的半群 S 的一个子集 S' 叫作 S 的一个 **子半群**, 若任取 $x,y\in S'$,$x*y\in S'$. 这时也称 *子集 $S'\subset S$ 关于运算 $*$ 封闭*. 若 $(M,*)$ 是一个幺半群，子集 $M'\subset M$ 不仅关于运算 $*$ 封闭，而且包含 M 的单位元，则 M' 叫作 M 的一个 *子幺半群*. 例如 $(n\mathbb{Z},\cdot)$ 是 $(\mathbb{Z},\cdot)$ 中的子半群，而 $(n\mathbb{Z},+,0)$ 是 $(\mathbb{Z},+,0)$ 中的子幺半群. 幺半群 $M(\Omega)$ 中的任意子幺半群叫作 (集合 Ω) 的 **变换幺半群**.

3. 广义结合律; 方幂 设 $(x,\cdot)$ 是任意一个带有二元运算 $\cdot$ 的代数结构，为了简便起见，我们将省去记号 $\cdot$, 用 xy 代替 $x\cdot y$. 设 $x_1,\cdots,x_n$ 是 X 中的一个有序列. 在不改变次序的前提下，我们可以有多种不同的方式构成长度为 n 的乘积. 设 l_n 是这些方式的个数:

$$
\begin{aligned}
l_2=1:&\quad x_1x_2;\\
l_3=2:&\quad (x_1x_2)x_3,\quad x_1(x_2x_3);\\
l_4=5:&\quad ((x_1x_2)x_3)x_4,\quad (x_1(x_2x_3))x_4,\\
&\quad x_1((x_2x_3)x_4),\quad x_1(x_2(x_3x_4)),\quad (x_1x_2)(x_3x_4);\\
&\quad \cdots\cdots\cdots\cdots
\end{aligned}
$$

显然，当 $1\leqslant k\leqslant n-1$ 时，分别找出 $x_1,\cdots,x_k$ 的所有可能的长度为 k 乘积和 $x_{k+1},\cdots,x_n$ 的所有可能的长度为 $(n-k)$ 的乘积，然后将其相乘，我们就穷尽了 l_n 种可能的乘积. 十分美妙的是，在幺半群 (和半群) 中，括号位置的选择是不必要的.

定理 1 *如果 X 上的二元运算是结合的，那么 X 中 n 个元素相乘的结果与括号的位置无关.*

证明 当 $n=1,2$ 时无需证明. 当 $n=3$ 时就是结合律. 进一步的论证要对 n 作归纳. 设 $n>3$, 并设当元素的个数 $<n$ 时，结论是正确的. 我们仅需指出

$$
(x_1\cdots x_k)(x_{k+1}\cdots x_n)=(x_1\cdots x_l)(x_{l+1}\cdots x_n) \tag{1}
$$

对任意 k,l 成立，其中 $1\leqslant k,l\leqslant n-1$. 我们仅给出了最外面的一对括号，因为根据归纳

条件,内部括号的位置是非本质的.特别地,乘积 $x_1x_2\cdots x_k = (\cdots((x_1x_2)x_3)\cdots x_{k-1})x_k$ 叫作 **左正规化的**. 区分两种情况:

a) $k = n-1$; 那么 $(x_1\cdots x_{n-1})x_n = (\cdots(x_1x_2)\cdots x_{n-1})x_n$, 后者是一个左正规化乘积;

b) $k < n-1$; 从结合律得到

$$\begin{aligned}&(x_1\cdots x_k)(x_{k+1}\cdots x_n) = (x_1\cdots x_k)((x_{k+1}\cdots x_{n-1})x_n)\\&\quad = ((x_1\cdots x_k)(x_{k+1}\cdots x_{n-1}))x_n = (\cdots((\cdots(x_1x_2)\cdots x_k)x_{k+1})\cdots x_{n-1})x_n,\end{aligned}$$

也得到一个左正规化乘积. 并且待证的等式 (1) 右侧亦可化为同样形式的乘积, 定理证毕. □

前面引入过求和号 $\sum x_i$. 它显然适用于任意的加法交换幺半群. 在乘法幺半群中, 有类似的求积号:

$$\prod_{i=1}^{2} x_i = x_1x_2, \quad \prod_{i=1}^{3} x_i = (x_1x_2)x_3, \quad \prod_{i=1}^{n} x_i = \left(\prod_{i=1}^{n-1} x_i\right)x_n.$$

根据定理 1, 幺半群的元素 $x_1, x_2, \cdots, x_n$ 的乘积在记法 (或计算) 中不必写括号. 唯一需要关注的是当元素彼此不交换时指明因子的顺序. 特别地, 当 $x_1 = x_2 = \cdots = x_n = x$ 时, 乘积 $x\,x\cdots x$ 就像数的运算那样记作 x^n, 称为元素 x 的 n **次方幂**. 从定理 1 可推出关系式

$$x^m x^n = x^{m+n}, \quad (x^m)^n = x^{mn}, \quad m, n \in \mathbb{N} \tag{2}$$

在幺半群 $(M, \cdot, e)$ 中, 对任意 $x \in M$, 仍令 $x^0 = e$.

在加法幺半群 $(M, +, 0)$ 中, 方幂 $x^n \in (M, \cdot, e)$ 对应于元素 x 的倍数 $nx = x + \cdots + x$. 公式 (2) 对应于倍数法则:

$$mx + nx = (m+n)x, \quad n(mx) = nmx. \tag{2'}$$

我们再指出一些有用的事实. 如果在幺半群 M 中有 $xy = yx$, 则

$$(xy)^n = x^n y^n, \quad n = 0, 1, 2, \cdots. \tag{3}$$

特别地, 该式在交换幺半群中永远成立, 公式 (3) 可对 n 作归纳证明:

$$\begin{aligned}(xy)^n &= (xy)^{n-1}(xy) = (x^{n-1}y^{n-1})(xy)\\&= (x^{n-1}y^{n-1}x)y = (x^{n-1}xy^{n-1})y = (x^{n-1}x)(y^{n-1}y)\\&= x^n y^n.\end{aligned}$$

更一般地, 若 $x_ix_j = x_jx_i, \quad i, j = 1, \cdots, m$, 运用 (3) 式并对 m 作归纳, 得到

$$(x_1\cdots x_m)^n = x_1^n \cdots x_m^n. \tag{4}$$

类似地，若 $x+y=y+x$ 且 $x_i+x_j=x_j+x_i, i,j=1,\cdots,m$, 则

$$n(x+y)=nx+ny,\quad n=0,1,2,\cdots \tag{3'}$$

$$n(x_1+\cdots+x_m)=nx_1+\cdots+nx_m,\quad n=0,1,2,\cdots \tag{4'}$$

一般来说，称 $(M,\cdot,e)$ 为 **乘法** 幺半群．而称 $(M,+,0)$ 为 **加法** 幺半群．在大多数情况下，只有当幺半群交换时才用加法记号.

4. 可逆元素 幺半群 $(M,\cdot,e)$ 的一个元素 a 称为 **可逆的**, 若存在元素 $b\in M$, 使得 $ab=e=ba$(显然元素 b 也是可逆的). 如果还有 $ab'=e=b'a$, 则 $b'=eb'=(ba)b'=b(ab')=be=b$. 这就为我们定义元素 $a\in M$ 的逆元 a^{-1} 奠定了基础：$a^{-1}a=e=aa^{-1}$.

不言而喻, $(a^{-1})^{-1}=a$. 幺半群中可逆元素的概念可以看作乘法幺半群$(M_n(\mathbb{R}),\cdot,E)$中可逆矩阵的自然推广.

因为 $(xy)(y^{-1}x^{-1})=x(yy^{-1})x^{-1}=xex^{-1}=e$, 类似地， $(y^{-1}x^{-1})(xy)=e$, 所以 $(xy)^{-1}=y^{-1}x^{-1}$. 于是，幺半群 $(M,\cdot,e)$ 中全体可逆元素的集合对运算封闭，并构成 M 中的一个子幺半群.

习 题

1. 作为一个例子在第 2 段中曾引出了 $\mathbb{Z}$ 上的运算 $*: n*m=-n-m$, 它是交换但非结合的. 在代数结构 $(\mathbb{Z},*)$ 中有恒等式 $(n*m)*m=n, m*(m*n)=n$. 现在假设给出一个任意的代数结构 $(X,*)$, 使得任取 $x,y\in X, (x*y)*y=x, y*(y*x)=x$. 证明 $x*y=y*x$, 即算子 $*$ 是交换的. 无需给出任何提示，因为这是本书中最没用的习题之一. 但毕竟还是个练习！

2. 证明集合

$$M_n^0(\mathbb{R})=\left\{A=(a_{ij})\in M_n(\mathbb{R})\,\middle|\,\sum_{j=1}^n a_{ij}=0,\quad i=1,2,\cdots,n\right\}$$

在矩阵的通常乘法运算下构成一个半群. $(M_n^0(\mathbb{R}),\cdot)$ 是幺半群吗？

3. 在乘法幺半群 M 中选出任意一个元素 t, 并引入一个新的运算 $*: x*y=xty$. 证明 $(M,*)$ 是一个半群，且 $(M,*)$ 成为一个幺半群，当且仅当所选的元素 t 是可逆的，这时它的单位元是 t^{-1}.

4. 证明集合 $\mathbb{Z}$ 关于运算 $\circ$ 构成一个交换幺半群，其中 $\circ: n\circ m=n+m+nm=(1+n)\times(1+m)-1$. 什么是 $(\mathbb{Z},\circ)$ 的单位元？找出 $(\mathbb{Z},\circ)$ 的全部可逆元.

§2 群

1. 定义和例子 考察行列式不为 0 的实系数 $n\times n$ 矩阵的集合 $\mathrm{GL}_n(\mathbb{R})$. 根据第 3 章 §2 的定理 3, $\det A\neq 0, \det B\neq 0\Rightarrow \det AB\neq 0$. 我们看到， $A,B\in\mathrm{GL}_n(\mathbb{R})\Rightarrow AB\in\mathrm{GL}_n(\mathbb{R})$. 进一步， $(AB)C=A(BC)$, 并且存在一个矩阵 E, 使得对

一切 $A\in \mathrm{GL}_n(\mathbb{R}),AE=EA=A$. 此外，任意矩阵 $A\in \mathrm{GL}_n(\mathbb{R})$ 都有 "逆元"，即逆矩阵 A^{-1}，使得 $AA^{-1}=A^{-1}A=E$.

集合 $\mathrm{GL}_n(\mathbb{R})$ 连同合成法则 (二元运算)$(A,B)\mapsto AB$ 称为 $\mathbb{R}$ 上的 **n 阶一般线性群**，沿用 §1 的术语，它是幺半群 $(M_n(\mathbb{R}),\cdot,E)$ 中的所有可逆元素构成的子幺半群. 但是这个子幺半群特别重要，它得到了特殊的命名，并成为一般理论有价值的实例.

定义 *所有的元素都可逆的幺半群叫作* **群**. *换言之，下述公理必须满足.*

G0) *在集合 G 上定义了一个二元运算 $(x,y)\mapsto xy$.*

G1) *运算是结合的：任取 $x,y,z\in G,(xy)z=x(yz)$.*

G2) *G 有单位元 e: 任取 $x\in G,xe=ex=x$.*

G3) *G 的任意元素 x 有逆元 x^{-1}:$xx^{-1}=x^{-1}x=e$.*

我们在第 1 章 §8 中引出的代数结构 S_n 满足上述公理，称之为 n 元置换的 *对称群*. 事实上，正是这些重要的例子，使我们想到了群的一般定义.

令人惊讶的是，代数学中最古老和结果最丰富的领域，竟然建立在这样一组简单的公理之上，这一领域在几何学中，以及将数学应用到自然科学当中发挥着根本作用. 稍加分析可见，它们还可以进行简化，但这种事对于我们来说不是原则性的.

带有交换二元运算的群自然叫作交换群，也常常叫作 **阿贝尔群**(为了纪念挪威数学家阿贝尔)."群" 这一术语是由群论的创始人，法国数学家伽罗瓦引入的. 群论的思想在伽罗瓦之前已有流传 (就像基本的数学思想产生时常有的那样)，拉格朗日实际上已经证明了群论的一些定理，虽然其形式是朴素的. 伽罗瓦天才的工作起初并没有被人们理解，对这一工作重又引起兴趣是在若尔当的书《置换与代数方程》(1870 年) 出版之后开始的. 直到 19 世纪末，群论才 "完全脱离了梦幻，代之以精细整理过的逻辑结构." (克莱因，《 19 世纪数学发展史讲义》).

对于群 G 中元素的个数 (更准确地说，群的基数)，可用等价的符号 $\mathrm{Card}G,|G|$，以及 $(G:e)$ 表示. 当然在 §1 中关于幺半群的全部论述都可以用到群上来. 仅需引入一些必要的新名词. 特别是，子集 $H\subset G$ 称为 G 的一个 **子群**，若 $e\in H;h_1,h_2\in H\Rightarrow h_1h_2\in H$; 且 $h\in H\Rightarrow h^{-1}\in H$. 子群 $H\subset G$ 叫作一个 **真子群**，若 $H\neq\{e\}$，且 $H\neq G$.

我们再给出一些群的例子.

例 1 在一般线性群 $\mathrm{GL}_n(\mathbb{R})$ 中考察由行列式为 1 的矩阵构成的子集 $\mathrm{SL}_n(\mathbb{R})$:

$$\mathrm{SL}_n(\mathbb{R})=\{A\in \mathrm{GL}_n(\mathbb{R})|\det A=1\}.$$

显然，$E\in \mathrm{SL}_n(\mathbb{R})$. 根据第 3 章关于行列式的一般结果

$$\det A=1,\ \det B=1\Rightarrow \det AB=1,$$
$$\det A^{-1}=(\det A)^{-1}=1.$$

所以 $\mathrm{SL}_n(\mathbb{R})$ 是 $\mathrm{GL}_n(\mathbb{R})$ 的一个子群；称为 $\mathbb{R}$ 上的 n 阶 **特殊线性群**. 它也叫作 **单位**

模群, 然而后一名词通常用于行列式为 ± 1 的矩阵构成的群.

应该指出，群 $\mathrm{GL}_n(\mathbb{R})$ 中包含着许多有趣的群，几代数学家都把它看作新的思想和未解决问题的无尽的源泉.

例 2　用有理数代替实数，我们就得到了 $\mathbb{Q}$ 上的 n 阶一般线性群 $\mathrm{GL}_n(\mathbb{Q})$ 及其子群 $\mathrm{SL}_n(\mathbb{Q})$, 在群 $\mathrm{SL}_n(\mathbb{Q})$ 中包含一个有趣的子群 $\mathrm{SL}_n(\mathbb{Z})$, 它由行列式为 1 的整数矩阵组成. 第 3 章 §3 的定理 1 给出了其逆矩阵的表达式, 由此可以证明，$\mathrm{SL}_n(\mathbb{Z})$ 确实是一个群. 群 $\mathrm{SL}_n(\mathbb{Q})$ 和 $\mathrm{SL}_n(\mathbb{Z})$ 在数论中占有重要的地位. 在图 15 中，$\mathrm{GL}_n(\mathbb{R})$ 的上述子群构成了一个偏序集 (见第 1 章 §6 第 4 段).

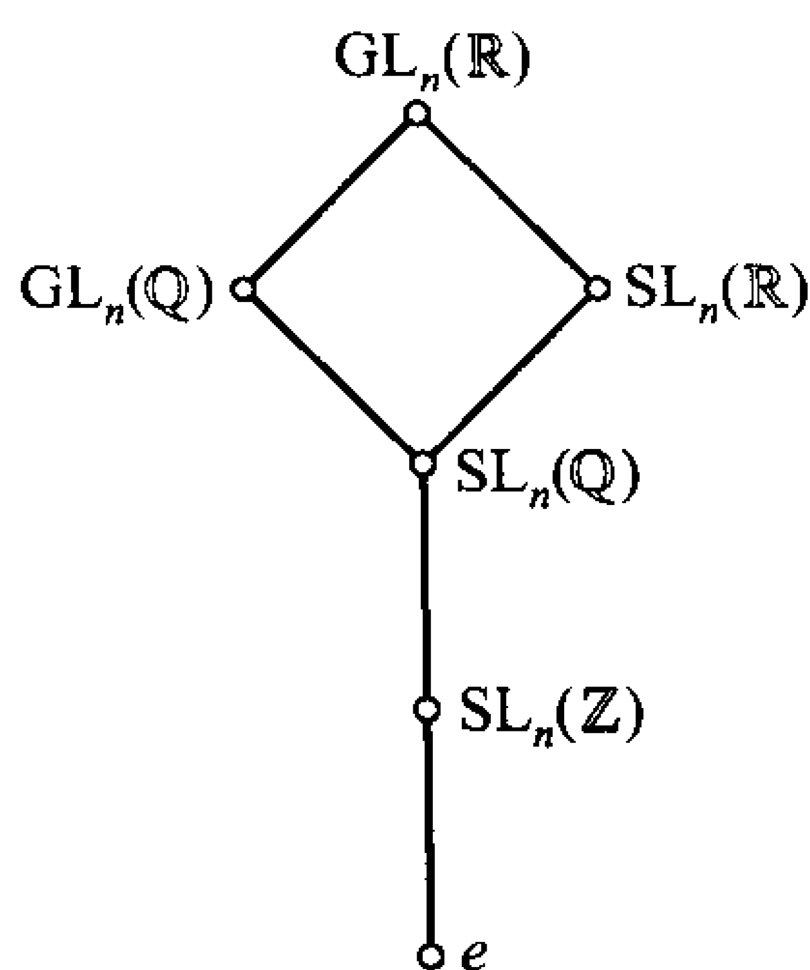


图 15

例 3　令例 1 和例 2 中的 $n=1$, 我们得到了实数和有理数上的 1 阶乘法群

$$\mathbb{R}^* = \mathbb{R}\backslash\{0\} = \mathrm{GL}_1(\mathbb{R}),\quad \mathbb{Q}^* = \mathbb{Q}\backslash\{0\} = \mathrm{GL}_1(\mathbb{Q}).$$

这些群显然是无限的. 因为在 $(\mathbb{Z},\cdot,1)$ 中的可逆元仅有 1 和 -1, 故 $\mathrm{GL}_1(\mathbb{Z}) = \{\pm 1\}$. 进一步，$\mathrm{SL}_1(\mathbb{R}) = \mathrm{SL}_1(\mathbb{Q}) = \mathrm{SL}_1(\mathbb{Z}) = 1$. 但当 $n=2$, 甚至连群 $\mathrm{SL}_2(\mathbb{Z})$ 都是无限的，比如：它包含所有的矩阵

$$\begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix},\quad \begin{pmatrix} 1 & 0 \\ m & 1 \end{pmatrix},\quad \begin{pmatrix} m & m-1 \\ 1 & 1 \end{pmatrix},\quad m \in \mathbb{Z}.$$

我们进一步指出若干无限加法群：

$$(\mathbb{R},\ +,\ 0),\ (\mathbb{Q},\ +,\ 0),\ (\mathbb{Z},\ +,\ 0).$$

例 4　设 Ω 是任意集合，而 $S(\Omega)$ 是全体双射 (一一映射)$f:\Omega\to\Omega$ 的集合. 考虑到第 1 章 §5 关于集合的映射的结果 (定理 1, 定理 2 以及定理 2 的推论), 我们马上断言，$S(\Omega)$ 是一个群，其自然的二元运算是映射的合成. 自然地，$S(\Omega)$ 是 §1 例 1 中定义的幺半群 $M(\Omega)$ 的子幺半群，它由 $M(\Omega)$ 的全体可逆元素组成，但这个细节我们就不过多强调了. 群 $S(\Omega)$ 自身，特别是它的各类子群叫作 *变换群*, 它们在群

论的各种应用中是很基础的. 1872 年克莱因宣布了著名的 "爱尔兰根纲领", 将变换群的概念作为对各种几何学进行分类的基础 (关于这一点详见 [BA II]).

如果将 Ω 取作线性空间 $\mathbb{R}^n$, 我们就得到了一个 "很大" 的难以全面认识的群 $S(\mathbb{R}^n)$. 但 $S(\mathbb{R}^n)$ 中包含一个由可逆线性变换 $\varphi_A: \mathbb{R}^n \to \mathbb{R}^n$ 构成的子群, 它与 n 阶非退化矩阵 A 一一对应 (见第 2 章 §3).

这样就可以把 $\mathrm{GL}_n(\mathbb{R})$ 嵌入到 $S(\mathbb{R}^n)$ 中.

在下面引入群同构的重要概念之后, 这一嵌入的含义就清楚了.

2. 循环群 设 G 是乘法群 (即带有乘法运算),a 是 G 的一个取定的元素. 如果任意元素 $g \in G$ 都可以写成 $g = a^n$ 的形式, 其中 $n \in \mathbb{Z}$, 则称 $G = \langle a \rangle$ 是带有生成元 a 的 **循环群**(或由元素 a 生成的循环群). 类似地, 在加法的情况下, 循环群定义成 $\langle a \rangle = \{na | n \in \mathbb{Z}\}$. 当然, 这并不意味着元素 a^n 或 na 是两两不同的. 约定符号 $(a^{-1})^k = a^{-k}$, 并证明下述论断的正确性.

定理 1 任取$m, n \in \mathbb{Z}$,

$$a^m a^n = a^{m+n}, \quad (a^m)^n = a^{mn}$$

(对应地, $ma + na = (m+n)a, \quad n(ma) = (nm)a$).

证明 如果 m, n 是非负的, 见 §1 第 3 段的关系式 (2) 和 (2′). 如果 $m < 0, n < 0$, 则 $m' = -m > 0, n' = -n > 0$, 且

$$a^m a^n = (a^{-1})^{m'} (a^{-1})^{n'} = (a^{-1})^{m'+n'} = a^{-(m'+n')} = a^{m+n}.$$

如果 $m' = -m > 0, \ n > 0$, 则有

$$a^m a^n = (a^{-1})^{m'} a^n = (\underbrace{a^{-1} \cdots a^{-1}}_{m'})(\underbrace{a \cdots a}_{n}) = a^{n-m'} = a^{m+n}.$$

如果 $m' \geqslant n$, 则

$$a^{n-m'} = (a^{-1})^{m'-n} = a^{m+n}.$$

当 $m > 0, n < 0$ 时, 可类似地处理. 利用上述论断和元素方幂的定义, 易证等式 $(a^m)^n = a^{mn}$. □

循环群最简单的例子是整数加群 $(\mathbb{Z}, +, 0)$, 它由元素 1 或 -1 生成. 易验证矩阵 $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ 生成 $\mathrm{SL}_2(\mathbb{Z})$ 的一个无限循环子群. 集合 $\{1, -1\}$ 是一个 2 阶的乘法循环群.

我们来看 n 阶循环群的一个例子, 考察平面绕某个点 O 的旋转, 使得中心在 O 点的任意正 n 边形 P_n 变到自身. 显然, 这些旋转构成一个群: 它的乘法是将两个旋转依次施行. 我们的群 C_n 含有旋转 $\varphi_0, \varphi_1, \cdots, \varphi_{n-1}$, 它们分别是依逆时针方向旋

转角度 0, $\frac{2\pi}{n}, \cdots, \frac{(n-1)2\pi}{n}$. 这时 $\varphi_s = \varphi_1^s$, 从几何直观出发, 显然有 $\varphi_s^{-1} = \varphi_1^{n-s}$, 且 $\varphi_1^n = \varphi_0$(单位变换). 于是 $|C_n| = n$ 且 $C_n = \langle\varphi_1\rangle$. 注意循环群 C_n 是正 n 边形 P_n 的全体对称变换 (即 P_n 到自身的变换)D_n 的一个真子群.

再一次假定 G 是任意群, a 是 G 的一个元素. 我们得到了两种可能性.

1) 元素 a 的所有方幂两两不同, 即 $m \neq n \Rightarrow a^m \neq a^n$. 这时称元素 a 是一个 **无限阶元**.

2) 当 $m \neq n$ 时, 有等式 $a^m = a^n$. 如果 $m > n$, 则 $a^{m-n} = e$, 即元素 a 的某个正方幂等于 G 的单位元. 设 q 是使 $a^q = e$ 的最小正数, 这时我们称元素 a 是 **有限阶元**, 阶数为 q.

在一个有限群 $G(\mathrm{Card}G < \infty)$ 中, 自然所有的元素都是有限阶的.

注意 "阶" 这个词在数学中有多种含义. 我们以前谈过 n 阶方阵 (即 $n \times n$ 阶的矩阵), 但一个非退化矩阵 A 作为 $\mathrm{GL}_n(\mathbb{R})$ 的元素也有在刚才指出的意义下的一个阶 (可能是无限的). 但从上下文看, 每一次出现的阶的含义都是清楚的.

回顾 n 阶循环群, 下述论断几乎是显然的.

定理 2 任意元素 $a \in G$(这里 G 是任意的群) 的阶等于 $\mathrm{Card}\langle a\rangle$. 如果 a 是一个 q 阶元, 则 $\langle a\rangle = \{e, a, \cdots, a^{q-1}\}$,

$$a^k = e \Leftrightarrow k = lq, \quad l \in \mathbb{Z}.$$

证明 如果 a 是无限阶元, 无需证明. 如果 a 是 q 阶元, 则由定义, 元素 $e, a, a^2, \cdots, a^{q-1}$ 两两不同. 任意其他的方幂 a^k 与这些元素之一重合, 即 $\langle a\rangle = \{e, a, \cdots, a^{q-1}\}$. 为此, 利用 $\mathbb{Z}$ 中的带余除法 (第 1 章 §9 第 3 段), 将 k 写成如下形式

$$k = lq + r, \quad 0 \leqslant r \leqslant q - 1$$

运用定理 1 给出的方幂法则, 得到

$$a^k = (a^q)^l\, a^r = ea^r = a^r.$$

特别地, $a^k = e \Rightarrow r = 0 \Rightarrow k = lq$. □

3. 同构 前面已经指出, 沿逆时针方向旋转 0°, 120°, 240° 的三个旋转 $\varphi_0, \varphi_1, \varphi_2$ 将等边三角形 P_3 变到自身. 但是还有图 16 指出的三个 轴对称变换 (反射)ψ_1, ψ_2, ψ_3. 它们的对称轴分别是 $1 — 1', 2 — 2', 3 — 3'$. 全体 6 个对称变换分别对应于三角形顶点集的六个置换. 我们得到

$$\begin{aligned} &\varphi_0 \sim e, \quad &&\varphi_1 \sim (123), \quad &&\varphi_2 \sim (132), \\ &\psi_1 \sim (23), \quad &&\psi_2 \sim (13), \quad &&\psi_3 \sim (12). \end{aligned}$$

因为不再有其他的三元置换, 故可断言, 正三角形的全体对称变换组成的群 D_3 显示出与对称群 S_3 的极大类似.

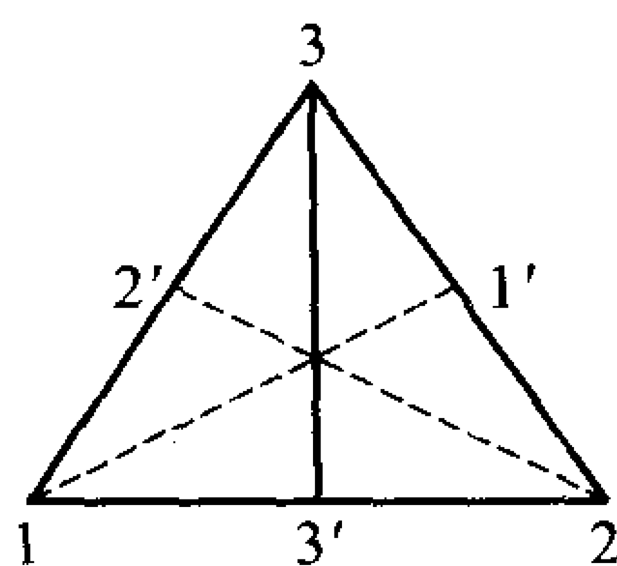


图 16

在同样的意义下，循环群 C_n(见第 2 节例) 和 $\langle(1\ 2\ \cdots\ n)\rangle \subset S_n$ 彼此相似. 这些事实和关于群的一般性思考，引出了一个十分自然的问题，它涉及群的最本质的属性. 初看起来，一个群 G 的全部信息已包含在 G 的乘法表中，称之为**凯莱表**:

	g_1	g_2	$\cdots$	g_n	$\cdots$
g_1	g_1g_1	g_1g_2	$\cdots$	g_1g_n	$\cdots$
g_2	g_2g_1	g_2g_2	$\cdots$	g_2g_n	$\cdots$
$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$
g_n	g_ng_1	g_ng_2	$\cdots$	g_ng_n	$\cdots$
$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$

事实上，群的很多规律可以从观察它的凯莱表得出，即从以 $m_{ij} = g_ig_j \in G$ 为元素的矩阵 $M = (m_{ij})$ 得出 (若 $n = (G : e)$, 矩阵的阶为 $n \times n$). 例如，我们注意到在矩阵 M 的每一行和每一列，群 G 的任意元素刚好出现一次 (见下述定理 4 的证明). 群 G 是阿贝尔群当且仅当矩阵 M 是对称的，即 $m_{ij} = m_{ji}$. 可以从表中得到的群的性质有很多，但是毕竟在比较两个群 G 和 G' 的乘法表时，涉及元素的排列顺序，因为矩阵 M 的形状依赖于群元素的取法，而在无限群的情形，情况就更加复杂.

比较群 G 与 G' 的最正确最基本的方法基于同构的概念.

定义 两个分别具有运算 $*$ 与 $\circ$ 的群 $(G, *)$ 与 $(G', \circ)$ 称为**同构**的，若存在一个映射 $f: G \to G'$, 使得

i) $f(a * b) = f(a) \circ f(b)$ 对任意 $a, b \in G$ 成立;

ii) f 是双射.

通常用符号 $G \simeq G'$ 表示两个群同构.

我们给出同构的一些简单性质.

1) 单位元对应到单位元. 事实上，若 e 是群 G 的单位元，则 $e * a = a * e = a$, 这就意味着 $f(e) \circ f(a) = f(a) \circ f(e) = f(a)$, 因而 $f(e) = e'$ 是群 G' 的单位元. 这一证明部分地用到了 f 的两个性质. 性质 i) 是显然的，性质 ii) 保证了 f 是满射，因而 $f(g)$ 取遍了群 G' 的所有元素.

2) $f(a^{-1}) = f(a)^{-1}$. 事实上，根据 1) $f(a) \circ f(a^{-1}) = f(a * a^{-1}) = f(e) = e'$ 是

G' 的单位元，从而

$$f(a)^{-1} = f(a)^{-1} \circ e' = f(a)^{-1} \circ (f(a) \circ f(a^{-1})).$$
$$= (f(a)^{-1} \circ f(a)) \circ f(a^{-1}) = e' \circ f(a^{-1}) = f(a^{-1}).$$

3) 逆映射 f^{-1}: $G' \to G$(根据性质 ii),f^{-1} 是存在的) 也是一个同构. 由于第 1 章 §5 定理 2 的推论，我们仅需验证 f^{-1} 满足性质 i). 设 a', $b' \in G'$. 由于 f 的双射性有 a, $b \in G$, 使 $f(a) = a'$, $f(b) = b'$. 因为 f 是同构， $a' \circ b' = f(a) \circ f(b) = f(a * b)$. 从而有 $a * b = f^{-1}(a' \circ b')$, 又因为 $a = f^{-1}(a')$, $b = f^{-1}(b')$, 故 $f^{-1}(a' \circ b') = f^{-1}(a') * f^{-1}(b')$.

注记 简单的验证表明，在群 D_3 和 S_3 之间建立的关系 $\sim$ 是一个同构.

函数 f: $= \ln$ 是正实数乘法群 $(\mathbb{R}_+, \cdot)$ 到全体实数的加法群 $(\mathbb{R}, +)$ 的一个同构映射. 显然对数函数的性质 $\ln ab = \ln a + \ln b$ 恰为同构定义中的性质 i) 的一个模型. f 的逆映射是指数函数 $x \mapsto e^x$.

现在我们来证明两个一般性的定理，说明同构在群论中的作用.

定理 3 任意两个同阶的循环群是同构的 (特别地，任意两个无限循环群是同构的).

证明 事实上，若 $\langle g \rangle$ 是无限循环群，则所有的 g 的方幂 g^n 是彼此不同的，令 $g^n \mapsto f(g^n) = n$, 我们得到了一个同构 f: $\langle g \rangle \to (\mathbb{Z}, +)$. f 的双射性是显然的，而性质 $f(g^m g^n) = f(g^m) + f(g^n)$ 由定理 1 推出.

现在设 $G = \{e, g, \cdots, g^{q-1}\}$, $G' = \{e', g', \cdots, (g')^{q-1}\}$ 是两个 q 阶循环群 (G 和 G' 中的运算均用乘法表示). 我们定义一个一一映射

$$f: g^k \mapsto (g')^k, \quad k = 0, 1, \cdots, q-1.$$

任取 $n, m = 0, 1, \cdots, q-1$, 设 $n + m = lq + r$, $0 \leqslant r \leqslant q-1$, 如同定理 2 的证明，我们有

$$f(g^{n+m}) = f(g^r) = (g')^r = (g')^{n+m} = (g')^n\, (g')^m = f(g^n)\, f(g^m). \qquad \square$$

定理 4(凯莱) 任意 n 阶有限群都同构于对称群 S_n 的某个子群.

证明 设 G 是我们的群， $n = |G|$. 可以将 S_n 看作集合 G 到自身的全体一一映射的集合，因为被 S_n 的置换所作用的那些元素，其自然属性是非本质的.

对于任意元素 $a \in G$, 我们来看由公式

$$L_a(g) = a\dot{g}$$

定义的映射 $L_a : G \to G$(显然我们重述了第 1 章 §8 第 3 段的定义). 如果 $e = g_1, g_2, \cdots, g_n$ 是群 G 的全部元素，那么 $ag_1, ag_2, \cdots, ag_n$ 是按照另外的次序排列

的 G 的全部元素 (回忆凯莱表). 这件事是明显的，因为

$$ag_i = ag_j \Rightarrow a^{-1}(ag_i) = a^{-1}(ag_j) \Rightarrow (a^{-1}a)g_i = (a^{-1}a)g_j \Rightarrow g_i = g_j.$$

显然， L_a 是一个双射 (置换), 其逆映射为 $L_a^{-1} = L_{a^{-1}}$. 恒等映射自然是 L_e.

再一次运用 G 中乘法的结合律，得到 $L_{ab}(g) = (ab)g = a(bg) = L_a(L_b\, g)$, 即 $L_{ab} = L_a\, L_b$.

令 $S(G)$ 是集合 G 到自身的全体双射组成的群,即群 S_n,则集合 L_e, L_{g_2}, $\cdots$, L_{g_n} 构成 $S(G)$ 的一个子群 H. 我们有包含关系 $H \subset S_n$ 和对应关系 $L : a \mapsto L_a \in H$, 根据上面的论述， L 具有同构的一切性质. □

凯莱定理虽然简单，但在群论中意义重大. 它引出了某种 “通用” 对象 (对称群 $\{S_n | n = 1, 2, \cdots\}$ 的族), 这种通用对象在精确到同构的意义下包含了所有的一般有限群. 短语 “精确到同构”, 即将所有同构的群归为一类，不仅反映出群论的本质也反映出整个数学的本质，没有这样的一般化，数学就失去了意义.

在同构的定义中若 $G' = G$, 我们就得到了群 G 到自身的同构映射 $\varphi : G \to G$. 称之为群的 **自同构**. 例如恒等映射 $e_G : g \mapsto g$ (以后简记作 1) 是自同构，但一般来说，群 G 也有非平凡自同构. 同构映射的性质 3) 表明，自同构的逆映射也是自同构. 如果 φ, ψ 是群 G 的自同构，那么任取 a, $b \in G$,$(\varphi \circ \psi)(ab) = \varphi(\psi(ab)) = \varphi(\psi(a)\, \psi(b)) = (\varphi \circ \psi)(a)\, (\varphi \circ \psi)(b)$. 事实上，群 G 的全体自同构的集合 $\mathrm{Aut}(G)$ 构成 $S(G)$ 的一个子群，后者由 $G \to G$ 的全体双射组成.

4. 同态 在群 G 的自同构群中含有一个特殊的子群. 它用符号 $\mathrm{Inn}(G)$ 表示，称为 **内自同构群**. 其元素是映射

$$I_a : g \mapsto aga^{-1}.$$

简单的练习表明， I_a 满足自同构的一切性质，并且 $I_a^{-1} = I_{a^{-1}}$, $I_e = 1$ 是单位自同构， $I_a \circ I_b = I_{ab}$(因为 $(I_a \circ I_b)(g) = I_a(I_b(g)) = I_a(b\, g\, b^{-1}) = abg\, b^{-1}\, a^{-1} = (ab)g(ab)^{-1} = I_{ab}(g)$).

最后一个关系式指出，由公式 $f(a) = I_a$, $a \in G$, 定义的从群 G 到它的内自同构群 $\mathrm{Inn}(G)$ 的映射

$$f : G \to \mathrm{Inn}(G)$$

满足自同构映射的性质 i):$f(a) \circ f(b) = f(ab)$. 但性质 ii) 不一定满足. 例如，当 G 是阿贝尔群时，任取 a, $g \in G$, $aga^{-1} = g$, 故 $I_a = I_e$, 群 $\mathrm{Inn}(G)$ 仅由单位元 I_e 组成. 这个例子自然导致了下述的一般化

定义 *群 $(G, *)$ 到 $(G', \circ)$ 的一个映射 $f : G \to G'$ 叫作* **同态映射**, *若*

$$\forall\, a,\, b \in G, \quad f(a * b) = f(a) \circ f(b)$$

(换言之，只满足同构定义中的性质 i)).

集合

$$\ker f = \{g \in G | f(g) = e', \text{其中} e' \text{是} G' \text{的单位元}\},$$

叫作同态 f 的 **核**.

群到自身的同态映射也叫作群的 **自同态**.

在同态的定义中不仅不要求 f 是单射，也不要求 f 是满射 (即 “到上” 的映射)，但这不是本质的，因为我们总可以局限于考察映射的像 $\operatorname{Im} f \subset G'$，它显然是 G' 的一个子群. 同态 f 与同构的主要区分点在于非平凡核 $\ker f$ 的存在性，它是度量 f 的非单射性的尺度. 如果 $\ker f = \{e\}$，则 $f : G \to \operatorname{Im} f$ 是一个同构.

我们指出

$$f(a) = e',\ f(b) = e' \Rightarrow f(a * b) = f(a) \circ f(b) = e' \circ e' = e', \text{且}$$

$$f(a^{-1}) = f(a)^{-1} = (e')^{-1} = e'.$$

所以核 $\ker f$ 是 G 的一个子群.

5. 术语. 例子 术语 满射(“到上” 的映射),**单射**(嵌入映射),**双射**(一一映射)，可用于任意集合间的映射 (不一定带有运算)，在讨论群 (或其他代数系统) 时，我们使用相应的术语满同态 (“到上” 的同态)，单同态 (带有单位核的同态)，同构 (一一同态，既满且单). 存在着用 **态射** 取代同态的倾向. 在阅读数学文献时了解这些术语是有用的，但最初读者 (如果愿意) 可以在术语同构与同态之前附加 “映入” 和 “映上” 等字样.

现在来进一步考察群同态的若干例子.

例 5 整数加群 $\mathbb{Z}$ 到 q 阶循环群 $\langle g \rangle$ 上有一个满同态映射 $f : n \mapsto g^n$(见 §2 定理 2). 此时，显然有 $\ker f = \{lq | l \in \mathbb{Z}\}$. 事实上，$\{lq\} \subset \ker f$ 是显然的，反面的包含关系从定理 1 得到.

例 6 从实数加群 $\mathbb{R}$ 到平面绕不动点 O 点的旋转群 T 的映射 $f : \mathbb{R} \to T$ 由公式 $f(\lambda) = \Phi_\lambda$ 给出 (此处 Φ_λ 是逆时针转过角度 $2\pi\lambda$ 的旋转)，它是一个同态，理由是 $\Phi_\lambda \circ \Phi_\mu = \Phi_{\lambda+\mu}$. 旋转 2π 的整倍数与单位旋转 (转零角度) 重合，故 $\ker f = \mathbb{Z}$. 也可以说 f 是 $\mathbb{R}$ 到单位圆周上的一个同态，因为在 Φ_λ 与单位圆周 S^1 的点之间存在一个由极坐标 $(1, 2\pi\lambda)$ 给出的一一对应，其中 $0 \leqslant \lambda < 1$.

例 7 一般线性群 $\mathrm{GL}_m(\mathbb{R})$ 由满足 $\det A \neq 0$ 的 $m \times m$ 实矩阵 A 构成，令 $f := \det$ 则有从 $\mathrm{GL}_m(\mathbb{R})$ 到非零实数乘法群 $\mathbb{R}^*$ 上的同态. 同态条件 $f(AB) = f(A)f(B)$ 恰为第 3 章 §2 定理 3 的公式. 根据定义 $\mathrm{SL}_m(\mathbb{R}) = \ker f$.

例 8 考察 2 阶循环群 $C_2 = \langle -1 \rangle = \{1, -1\}$. 如果必要，它可以用凯莱表抽象地给出：

C_2:

·	1	−1
1	1	−1
−1	−1	1

由已知的函数 $\varepsilon = \mathrm{sgn} : \pi \mapsto \varepsilon_\pi$(置换 π 的符号) 给出的映射 $\varepsilon : S_n \to C_2$ 是对称群 S_n 到 C_2 上的同态. 核 $\ker\varepsilon = A_n$, 阶为 $\dfrac{1}{2}n!$ (见第 1 章 §8 第 3 段),A_n 叫作*交错群*.

例 9 无限群可以同构于自己的真子群. 例如加法群 $(\mathbb{Z}, +)$ 包含有真子群 $n\,\mathbb{Z} = \{nk|k \in \mathbb{Z}\}$, 其中 $n > 1$ 是一个固定整数. 易验证由 $g_n(k) = nk$ 定义的映射 $g_n : \mathbb{Z} \to n\mathbb{Z}$ 是一个同构. 顺便指出, $\mathbb{Z}$ 和 $n\mathbb{Z}$ 都是无限循环群, 生成元分别为 1 或 −1, 以及 n 或 $-n$; 所以 g_n 和映射 $k \mapsto -nk$ 是 $\mathbb{Z} \to n\mathbb{Z}$ 的全部可能的同构映射.

例 10 群 $\mathrm{Aut}(G)$, 甚至个别的一个非单位元 $\varphi \in \mathrm{Aut}(G)$, 都可能带来群 G 的重要信息. 下面的例子可以说明这一点. 设 G 是有限群, 它有一个 2 阶自同构 $\varphi(\varphi^2 = 1)$, 没有非平凡的不动点:

$$a \neq e \Rightarrow \varphi(a) \neq a.$$

设 $\varphi(a)\,a^{-1} = \varphi(b)b^{-1}$ 对任意 $a,\ b \in\ G$ 成立. 对等式左乘 $\varphi(b)^{-1}$, 右乘 a, 得到 $\varphi(b)^{-1}\varphi(a) = b^{-1}a$, 即 $\varphi(b^{-1}a) = b^{-1}a$, 从而 $b^{-1}a = e,\quad b = a$. 也就是说, 当 a 取遍 G 的所有元素时, $\varphi(a)a^{-1}$ 亦然, 或等价地说, 任意元素 $g \in G$ 可以写成 $g = \varphi(a)a^{-1}$ 的形式. 但这时 $\varphi(g) = \varphi(\varphi(a))\varphi(a^{-1}) = \varphi^2(a)\varphi(a^{-1}) = a\ \varphi(a)^{-1} = (\varphi(a)a^{-1})^{-1} = g^{-1}$. 即 φ 重合于映射 $g \mapsto g^{-1}$. 由此得到 $ab = \varphi(a^{-1})\varphi(b^{-1}) = \varphi(a^{-1}\,b^{-1}) = (a^{-1}\,b^{-1})^{-1} = ba$, 即 G 是阿贝尔群. 此外 $(G:e)$ 是一个奇数, 因为 G 是由 e 和互不相同的元素对 $g_i, g_i^{-1} = \varphi(g_i)$ 组成的.

例 11 下述例子表明, 可以改变群的运算, 但在同构的意义下不改变群自身, (亦见 §1 习题 3). 设 G 是任意群, t 是 G 的一个给定的元素. 赋予集合 G 一个新的运算

$$(g,h) \mapsto g * h = gth.$$

我们可以直接验证 $(g_1 * g_2) * g_3 = g_1 * (g_2 * g_3)$, 即运算 $*$ 是结合的. 此外 $g * t^{-1} = t^{-1} * g = g$, 且 $g * (t^{-1}g^{-1}t^{-1}) = (t^{-1}g^{-1}t^{-1}) * g = t^{-1}$, 这就表明 $(G,*)$ 是带有单位元 $e_* = t^{-1}$ 的群. g 在 $(G,*)$ 中的逆元由 $g_*^{-1} = t^{-1}g^{-1}t^{-1}$ 给出. 映射 $f : g \mapsto gt^{-1}$ 建立了群 $(G,\cdot)$ 与 $(G,*)$ 之间的同构, 即 $f(gh) = f(g) * f(h)$.

上述所有的例子都说明了一个一般性的原则: 对群 G 的态射的研究反映出群 G 自身的重要信息.

习 题

1. 证明群 G 的任意子群族 $\{H_i|i \in I\}$ 的交 $\bigcap\limits_{i\in I} H_i$ 是 G 的一个子群.

2. 设 S 是群 G 的子集, 称 G 是由 S 生成的, 并记作 $G = \langle S\rangle$, 若包含 S 的所有子群的交

与 G 重合. (换言之, 在 G 中没有包含 S 的真子群.) 证明, 当 $G=\langle S\rangle$ 时, 任意元素 $g\in G$ 形如 $g=t_1t_2\cdots t_n$, $n=1,2,\cdots$, 其中 $t_i\in S$ 或 $t_i^{-1}\in S$, $1\leqslant t\leqslant n$.

3. 证明群 G 中乘法可换的元素 a,b 若有互素的阶 s,t, 则在 G 中生成一个 st 阶的循环子群: $\langle a,b\rangle=\langle ab\rangle$.

提示: 包含关系 $\langle ab\rangle\subset\langle a,b\rangle=\{a^i\ b^j|0\leqslant i\leqslant s-1,\ 0\leqslant j\leqslant t-1\}$ 显然成立. 根据第 1 章 §9 第 3 段, 从 $(s,t)=1$ 可知, 存在 $k,\ l\in\mathbb{Z}$, 使 $tk+sl=1$. 考虑到定理 1,$a=a^{1-sl}=a^{tk}=a^{tk}b^{tk}=(ab)^{tk}\in\langle ab\rangle$. 类似地, $b\in\langle ab\rangle$, 故 $\langle a,b\rangle\subset\langle ab\rangle$.

4. 设 $M=\langle S\rangle$ 是由集合 S 生成的幺半群, 如果每个元素 $s\in S$ 在 M 中可逆, 证明 M 是一个群.

5. 证明下述论断: 设 G 是一个幺半群, 使得任取 $a,\ b\in G$, 方程 $ax=b$, $ya=b$ 有唯一解, 则 G 是一个群.

6. 令 $\varphi_{a,b}:x\mapsto ax+b(a,\ b\in\mathbb{R};\ a\neq 0)$ 是 实直线上的一个**仿射变换**, 它们的集合记作 $A_1(\mathbb{R})$, 在 $A_1(\mathbb{R})$ 中定义乘法 $\varphi_{a,b}\varphi_{c,d}=\varphi_{ac,ad+b}$, 证明 $A_1(\mathbb{R})$ 是一个群. $A_1(\mathbb{R})$ 包含有一个子群 $\mathrm{GL}_1(\mathbb{R})$, 它使点 $x=0$ 保持不动, 也包含有一个由 "纯位移"$x\mapsto x+b$ 组成的子群.

7. 群 $\mathrm{SL}_2(\mathbb{Z})$ 包含有元素 $A=\begin{pmatrix}0&1\\-1&0\end{pmatrix}$ 和 $B=\begin{pmatrix}0&1\\-1&-1\end{pmatrix}$, 阶数分别为 4 和 3. 证明 $\langle AB\rangle$ 是 $\mathrm{SL}_2(\mathbb{Z})$ 中的无限循环子群. 这说明群 G 中两个有限阶元素的乘积不一定是有限阶元. 这件事在阿贝尔群中成立吗?

8. 证明若群 G 的阶 $|G|=2n$ 是一个偶数, 则 G 中包含有一个二阶元 $g\neq e$.

提示: 观察 G 用元素对 $g,\ g^{-1}$ 的划分.

9. 证明 $S_n=\langle(12),\ (13),\ \cdots,\ (1n)\rangle$.

10. 证明 $S_n=\langle(12),\ (123\ \cdots\ n)\rangle$.

11. 证明交错群 A_n, $n\geqslant 3$, 是由 3 循环生成的, 并且事实上

$$A_n=\langle(123),\ (124),\ \cdots,\ (12n)\rangle.$$

12. 证明循环 $\pi=(12\ \cdots\ n)\in S_n$ 的 k 次方幂 π^k 是 d 个互不相交的循环的乘积, 每一个的长度为 $q=n/d$, 其中 $d=\mathrm{g.c.d}(n,k)$ 是 n 和 k 的最大公因数.

13. 设置换 $\pi\in S_n$, 将 π 分解成互不相交的循环的乘积, 证明 π 的阶 (即循环子群 $\langle\pi\rangle$ 的阶), 等于这些循环的阶的最小公倍数.

14. 设 $A,\ B\in M_n(\mathbb{R})$ 且 $(AB)^m=E$ 对某个整数 m 成立, 那么一定有 $(BA)^m=E$ 吗?

15. 设 G 是一个有限 (乘法) 群, H 是 G 的一个非空子集, 如果 H 关于 G 的乘法封闭, 证明 H 是一个子群. 事实上, 在这种情况下, 在 H 中存在单位元 e 和逆元 $h^{-1}, h\in H$ 的要求是多余的.

16. 正有理数的乘法群 $(\mathbb{Q}_+,\ \cdot)$ 可以有什么样的生成元集?

提示: 利用第 1 章 §9 的算术基本定理.

在 $(\mathbb{Q}_+,\ \cdot)$ 中是否存在有限生成元集?

17. 证明对于给定的阶数 n, 在同构的意义下仅有有限多个 n 阶群, 群的个数记作 $\rho(n)$.

提示: 估计上述 n 阶凯莱表的个数. 运用定理 4 证明 $\rho(n)$ 不会超过 $\begin{pmatrix}n!\\n\end{pmatrix}$, 即从 S_n 中取 n 个置换组成的不同子集的个数. 事实上, $\rho(n)$ 远小于此数, 但逼近于精确值的较好的估计

至今没有找到.

18. 用习题 10 证明, 每个有限群都可以嵌入到具有两个生成元的有限群中 (即存在到这种群内的一个单同态).

19. 试证图 17 标示出了交错群 A_4 的所有子群.

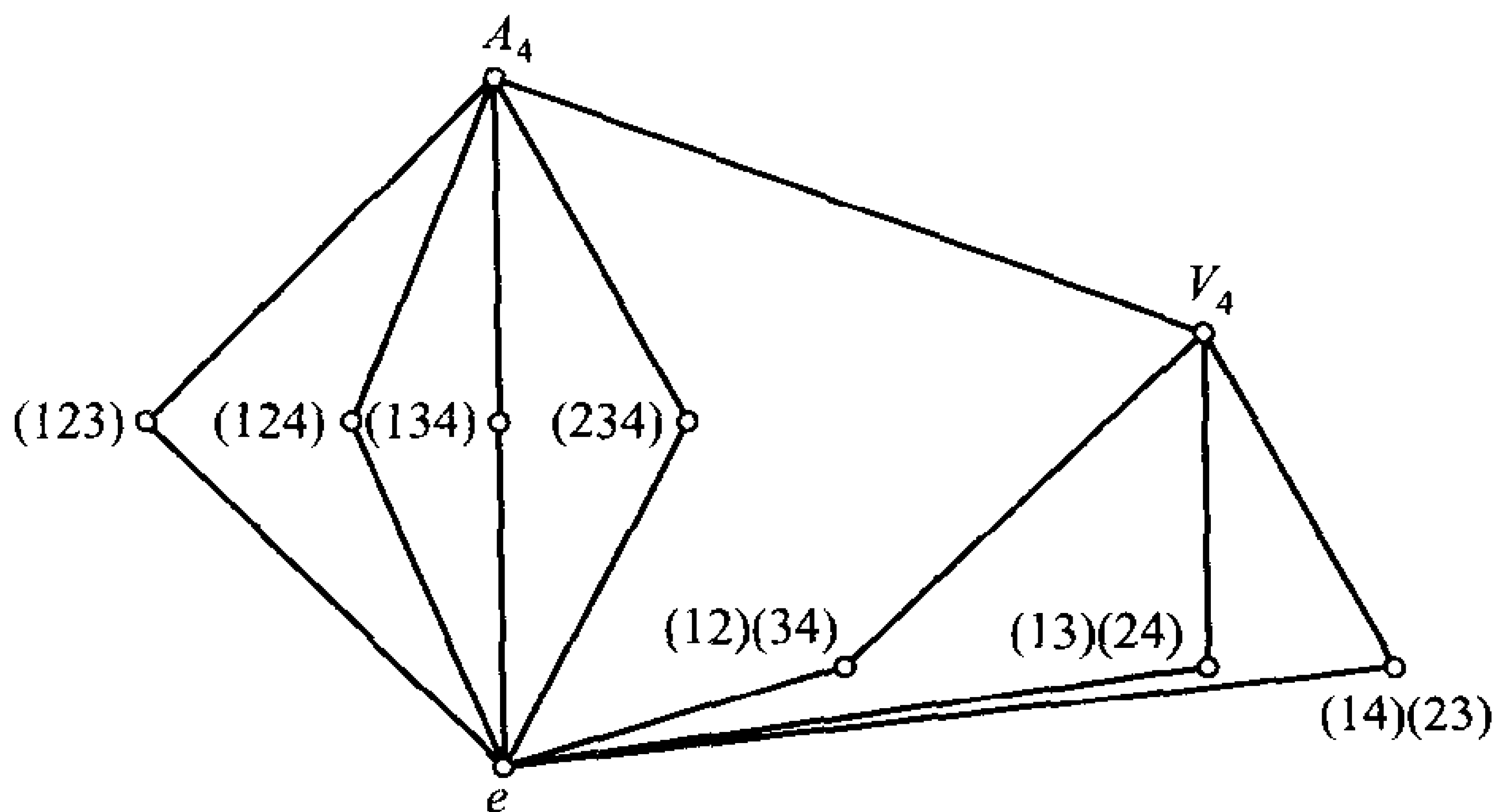


图 17

其中符号 V_4 代表克莱因 4 元群, $V_4 = \{e,\ (12)\ (34),\ (13)(24),\ (14)(23)\}$, 图中的其他顶点代表循环子群, 其生成元已写明.

20. 证明所有的 4 阶群都是阿贝尔群, 精确到同构只有置换群 $U = \langle(1234)\rangle$ 和克莱因四元群 V_4 两种, 也可以写成矩阵群:

$$L_1 = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \right\} \subset \mathrm{GL}_2(\mathbb{R}),$$

$$L_2 = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \right\} \subset \mathrm{GL}_2(\mathbb{R}).$$

给出同构映射 $U \to L_1$, $V_4 \to L_2$.

提示: 若任取 $x \in G$, 有 $x^2 = e$, 则 $abab = e \Rightarrow ab = b^{-1}a^{-1} = b(b^{-1})^2(a^{-1})^2a = beea = ba$.

§3 环和域

1. 环的定义和一般性质 代数结构 $(\mathbb{Z}, +)$,$(\mathbb{Z}, \cdot)$ 是最先进入我们视线的幺半群的例子. 后来看到 $(\mathbb{Z}, +)$ 是加法阿贝尔群 (事实上是循环群). 但人们经常把这两个结构合并在一起, 得到一个在数学上称之为环的代数结构. 初等算术最重要的两种运算的关系依赖于分配律 $(a+b)c = ac+bc$, 表面看来它很平凡, 那是因为我们已经习惯于它的存在. 如果我们试图, 例如, 将代数结构 $(\mathbb{Z}, +)$ $(\mathbb{Z}, \circ)$ 联系在一起, 其中 $n \circ m = n+m+nm$, 就会发现找不到在两个二元运算之间如此之好的协调性. 在列举更多的例子之前, 先给出环的精确定义.

定义 设 R 是一个非空集合, 在 R 上定义了两种 (二元代数) 运算 $+$(加法) 和 $\cdot$ (乘法), 满足下述条件:

R1) $(R,+)$ 是阿贝尔群;

R2) $(R,\cdot)$ 是半群;

R3) 加法和乘法运算以分配律相联系 (换言之, 乘法对加法的分配律), 即

$$(a+b)c = ac+bc, \ \ c(a+b) = ca+cb$$

对任意的 $a, b, c \in R$ 成立.

则称 $(R, +, \cdot)$ 是一个 **环**.

$(R, +)$ 叫作 **环的加法群**, 而 $(R, \cdot)$ 叫作它的 **乘法群**. 如果 $(R, \cdot)$ 是一个幺半群, 则称 $(R, +, \cdot)$ 是 **有单位元的环**.

环的单位元通常简记作 1. 1 的存在性有时列入环的定义中, 但我们不这样做.

在应用中和广义环论中 (这一理论正在蓬勃发展), 人们有时研究另外的代数结构. 其中条件 R2) 或是取消, 或是视具体问题代之以其他条件. 在这种情况下, 称它为 **非结合环**. 但我们在这里只考虑通常的 (结合) 环. 这就意味着我们可以根据 §1 的定理 1, 不必在意环中任意 k 个元素的乘积中括号的位置.

环 R 的子集 L 叫作一个 **子环**, 如果

$$\forall\, x, \, y \in L \Rightarrow x-y \in L \quad 和 \quad xy \in L,$$

也就是说, L 是环的加法群的子群和乘法半群的子半群.

显然, 环 R 的任意一簇子环的交仍然是一个子环 (证法与 §2 的习题 1 同), 于是谈论由 子集$T \subset R$生成的子环$\langle T\rangle \subset R$ 是有意义的. 根据定义, $\langle T\rangle$ 是 R 中包含有 T 的所有的子环之交. 如果 T 自身已经是一个子环, 则 $\langle T\rangle = T$.

如果任取 $x, y \in R$, 有 $xy = yx$, 则环 R 叫作 **交换的**(与群不同, 交换环通常不称作阿贝尔的).

环的概念是非常广泛的. 不仅如此, 初看起来非常特殊的交换环类是几十年来强有力的研究课题, 并且交换环论目前已与代数几何交织在一起, 后者是界于代数、几何和拓扑之间的一个漂亮的数学分支.

例 1 $(\mathbb{Z}, +, \cdot)$ 是带有通常的加法和乘法运算的 **整数环**. 能被 m 整除的整数集 $m\,\mathbb{Z}$ 是 $\mathbb{Z}$ 中的一个子环 (当 $m>1$ 时没有单位元). 类似地, $\mathbb{Q}$ 和 $\mathbb{R}$ 也是有单位元的环, 且包含关系 $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$ 给出了环 $\mathbb{R}$ 中的一个子环列.

例 2 我们在第 2 章中引进并详细讨论过 $M_n(\mathbb{R})$, n 阶方阵加法和乘法的性质表明, $M_n(\mathbb{R})$ 是一个有单位元 $1 = E$ 的环. 称之为 $\mathbb{R}$ 上的 全矩阵环, 也叫作 $\mathbb{R}$上的n 阶方阵环 (或 $\mathbb{R}$ 上 $n \times n$ 阶的矩阵环). 因为当 $n>1$ 时, 矩阵的乘法是不交换的, $M_n(\mathbb{R})$ 是一个非交换环. 元素取自 $\mathbb{Q}$ 和 $\mathbb{Z}$ 的同样阶数的方阵 $M_n(\mathbb{Q})$ 和 $M_n(\mathbb{Z})$ 分别是 $M_n(\mathbb{R})$ 的子环. 一般地, $M_n(\mathbb{R})$ 中饱含着各种各样的子环. 它们将不断地以自然的方式出现在我们的教程中. 我们进一步指出, 也可考察任意交换环 R 上的 n 阶方阵环 $M_n(R)$, 因为任意两个矩阵 $A, B \in M_n(R)$ 在相加和相乘后仍然是元素

取自 R 的矩阵, $M_n(R)$ 中的分配律可由 R 的分配律得到. 这些都可以从第 2 章 §3 的第 3 段和第 5 段所列的矩阵运算法则中直接推导出来.

例 3 除矩阵环外, 在各个数学领域中, **函数环** 亦有广泛的应用. 设 X 是任意集合, R 是任意环. 进一步设 $R^X = \{X \to R\}$ 是所有函数 (或映射) $f: X \to R$ 组成的集合, 如下定义两个二元运算 —— 逐点相加 $f+g$ 和逐点相乘 fg,

$$\begin{aligned}(f+g)(x) &= f(x) \oplus g(x),\\ (fg)(x) &= f(x) \odot g(x)\end{aligned}$$

(其中 $\oplus$ 和 $\odot$ 分别表示 R 当中的加法和乘法运算). 显然, 这不是函数的合成, 在线性映射的情况下, 合成法则导致了环 M_n. 而我们在这里建立的逐点相加和逐点相乘, 反映了数学分析的观点, 例如当 $X=\mathbb{R}$, $R=\mathbb{R}$ 时, 函数 tg 和 sin 的乘积为 $\mathrm{tg}\cdot\sin: x \mapsto \mathrm{tg}\, x \cdot \sin\, x$, 而不是 $\mathrm{tg}\circ\sin: x \mapsto \mathrm{tg}(\sin\, x)$.

容易验证 R^X 满足环的所有条件. 比如根据 R 中运算的分配律, 我们有

$$[f(x) \oplus g(x)] \odot h(x) = f(x) \odot h(x) \oplus g(x) \odot h(x)$$

对任意三个函数 $f, g, h \in R^X$ 和任意 $x \in X$ 成立, 根据逐点运算的定义, 这就给出了 $(f+g)h = fh+gh$. 第二个分配律的正确性可类似建立. 若 0,1 是 R 中的零元和单位元, 则 *常函数*

$$0_X: x \mapsto 0, \quad 1_X: x \mapsto 1$$

分别是 R^X 中的零元和单位元. 如果环 R 是交换的, 则函数环 R^X 也是交换的.

环 R^X 中包含各类子环, 它们可以用函数的各种特殊性质来定义. 例如, 设 $X=[0,1]$ 是 $\mathbb{R}$ 中的一个闭区间, 且 $R=\mathbb{R}$, 令 $\mathbb{R}^{[0,1]}$ 是定义在 [0,1] 区间上的所有实值函数环, 它包含有有界函数组成的子环 $\mathbb{R}_{\mathrm{b}}^{[0,1]}$, 连续函数的子环 $\mathbb{R}_{\mathrm{c}}^{[0,1]}$, 连续可微函数的子环 $\mathbb{R}_{\mathrm{d}}^{[0,1]}$, 等等, 因为所列举的性质都在函数的加法 (减法) 和乘法下保持下来.

任取 $a \in \mathbb{R}$, 定义一个常函数 $a_X: x \mapsto a$, $\forall x \in X$, 那么嵌入映射 $a \mapsto a_X$ 使我们可以将 $\mathbb{R}$ 看作 $\mathbb{R}^X$ 的一个子环. 总之, 几乎每一个自然的函数类都对应于 $\mathbb{R}^X$ 中的一个子环.

例 4 令 $(A,+)$ 是一个加法阿贝尔群, 任取 $x, y \in A$, 法则 $xy=0$ 建立了 A 的一个 **零乘法环结构**.

环的很多性质平行于群的对应的性质, 更一般地说, 平行于带有结合运算的集合的性质. 例如对所有的非负整数 m, n 和 $a \in R$, $a^m a^n = a^{m+n}$, $(a^m)^n = a^{mn}$ (与 §1 的公式 (2) 相比较). 而由环的定义中的三个条件导出的环的其他更特殊的性质可以从 $\mathbb{Z}$ 的性质得到启示. 我们列举其中的几条. 首先对任意 $a \in R$,

$$a \cdot 0 = 0 \cdot a = 0. \tag{1}$$

事实上，$a+0=a \Rightarrow a(a+0)=aa \Rightarrow a^2+a\cdot 0=a^2 \Rightarrow \quad a^2+a\cdot 0=a^2+0 \Rightarrow$ $a\cdot 0=0$(类似地，$0\cdot a=0$).

现在假定 $0=1$, 则任取 $a\in R$ 我们得到 $a=a\cdot 1=a\cdot 0=0$, 即 R 中仅有零元，因而在非平凡的环中，永远有 $0\neq 1$, 其次我们有

$$(-a)\cdot b=a(-b)=-(ab), \tag{2}$$

这是因为，例如，从 (1) 和分配律推出

$$0=a\cdot 0=a(b-b)=ab+a(-b)\Rightarrow a(-b)=-(ab). \tag{3}$$

因为 $-(-a)=a$, 由 (2) 得到等式 $(-a)(-b)=ab$ (例如 $(-1)(-1)=1$), 和 $-a=(-1)\cdot a$.

从分配律可以得到 **广义分配律**

$$(a_1+\cdots+a_n)(b_1+\cdots+b_m)=\sum_{i=1}^{n}\sum_{j=1}^{m}a_ib_j \tag{4}$$

证明并不困难，先令 $m=1$ 对 n 作归纳，然后再对 m 作归纳. 现在利用 (1),(2) 和 (3) 式得到

$$n(ab)=(na)b=a(nb)$$

对任意 $n\in\mathbb{Z}$ 和 $a,b\in R$ 成立.

最后我们指出，任取 $a,b\in R$, 牛顿二项式公式

$$(a+b)^n=\sum_{i=0}^{n}\begin{pmatrix} n\\ i\end{pmatrix}a^ib^{n-i} \tag{5}$$

仅当 R 是交换环时成立. 在 (5) 式的证明中需要用到 (4), 类似于在第 1 章 §7 中对特殊情况 $R=\mathbb{Z}$ 的处理.

2. 同余式. 剩余类环　设 m 是给定的自然数，$m>1$. 集合 $m\mathbb{Z}$ 显然不仅在加法运算下封闭，也在乘法运算下封闭，并满足环的定义中的三个条件.

现在我们来利用子环 $m\mathbb{Z}\subset\mathbb{Z}$, 构造一个只含有限个元素的非零环. 为此引入

定义　两个整数 n,n' 称为 **模m同余**, 若用 m 去除它们时余数相等. 记作 $n\equiv n'(m)$ 或 $n\equiv n'(\mathrm{mod} m)$, 这个式子叫作 **模$m$的 同余式**.

这样 $\mathbb{Z}$ 就被划分为数的类，每一类中的数模 m 同余，称之为模 m 的 **剩余类**. 每个剩余类形如

$$\{r\}_m=r+m\mathbb{Z}=\{r+mk|k\in\mathbb{Z}\},$$

因而

$$\mathbb{Z}=\{0\}_m\bigcup\{1\}_m\bigcup\cdots\bigcup\{m-1\}_m. \tag{6}$$

根据定义, $n \equiv n'(m) \Leftrightarrow n - n'$ 被 m 整除. 将关系式 $m|(n-n')$ 写成同余式 $n \equiv n'(m)$ 更加方便, 这些同余式可以进行通常的等式运算. 若 $k \equiv k'(m)$, 且 $l \equiv l'(m)$, 则 $k \pm l \equiv k' \pm l'(m)$, $kl \equiv k'l'(m)$. 特别地 $k \equiv k'(m) \Rightarrow ks \equiv k's(m)$ 对任意 $s \in \mathbb{Z}$ 成立.

这样, 可以对任意两个类 $\{k\}_m$ 和 $\{l\}_m$ 定义和或积, 所得结果是与代表元 k, l 的选取无关的类, 也就是说, 在模 m 的剩余类的集合 $\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z}$ 上诱导了唯一确定的运算 $\oplus$ 和 $\odot$:

$$\begin{aligned} \{k\}_m \oplus \{l\}_m &= \{k+l\}_m, \\ \{k\}_m \odot \{l\}_m &= \{kl\}_m. \end{aligned} \tag{7}$$

由于这些运算归结为对取自剩余类中的数的相应运算, 即在 $\mathbb{Z}$ 的元素上的运算, 故 $\{\mathbb{Z}_m, \oplus, \odot\}$ 也是一个带有单位元 $\{1\}_m = 1 + m\mathbb{Z}$ 的交换环. 称为**模 m 的剩余类环**. 当下标 m 固定时, 习惯于用 $\bar{k}$ 代替 $\{k\}_m$, 故

$$\begin{aligned} \bar{k} \oplus \bar{l} &= \overline{k+l}, \\ \bar{k} \odot \bar{l} &= \overline{kl}. \end{aligned}$$

在 $\mathbb{Z}_m$ 当中用代表元代替剩余类乍看起来是不严肃的, 但它的明显的技术上的优势在于, 放弃上横线和花括号, 仅依赖于模 m 代表元的某个确定集合, 通常取集合 $\{0, 1, 2, \cdots, m-1\}$, 称之为**模 m 的剩余类的导出集**. 在这一约定下, 我们有比如 $-k = m - k$, $2(m-1) = -2 = m-2$.

于是, 有限环是存在的. 我们给出三个简单的例子, 指明它们的加法表和乘法表:

$\mathbb{Z}_2$:

+	0	1
0	0	1
1	1	0

·	0	1
0	0	0
1	0	1

$\mathbb{Z}_3$:

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

·	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

$\mathbb{Z}_4$:

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

·	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

剩余类环 $\mathbb{Z}_m$ 很久以来就是数论学家感兴趣的对象, 而在代数中, 它是各类一般概念的出发点.

3. 环的同态 根据 (7) 式，映射 $f: n \mapsto \{n\}_m$ 有下述性质:

$$f(k+l) = f(k) \oplus f(l), f(kl) = f(k) \odot f(l).$$

这就使得我们可以在下述的一般定义下称环 $\mathbb{Z}$ 与 $\mathbb{Z}_m$ 为同态.

定义 设 $(R, +, \cdot)$ 和 $(R', \oplus, \odot)$ 是两个环. 映射 $f: R \to R'$ 称为 **同态**, 若 f 保持环的两种运算，即

$$f(a+b) = f(a) \oplus f(b),$$
$$f(ab) = f(a) \odot f(b).$$

这时易见， $f(0) = 0'$, 且 $f(na) = nf(a), n \in \mathbb{Z}$.

集合

$$\ker f = \{a \in R | f(a) = 0'\}$$

叫作同态 f 的 **核**. 显然 $\ker f$ 是 R 的一个子环.

与群的情况一样 (见 §2 第 5 段的术语), 同态

$$f: R \to R'$$

称为:

单同态, 若 $\ker f = 0$;

满同态, 若像与 R' 重合，即

$$\mathrm{Im} f = f(R) = \{a' \in R' | a' = f(a)\} = R';$$

同构, 若映射 f 既单且满.

两个环同构这一事实简短地记作 $R \cong R'$.

考察前面给出的映射 $f: n \mapsto \{n\}_m, f$ 显然是一个核为 $\ker f = m\mathbb{Z}$ 的满同态 $\mathbb{Z} \to m\mathbb{Z}$.

如果仅仅考察带有单位元的环，那么需要在同态 $f: R \to R'$ 中合理地加入条件

$$f(1) = 1'.$$

在满同态和同构的情况下，这个条件是自然满足的.

同构的环具有相同的代数性质，而数学上的真正兴趣在于环的那些在同构映射下保持不变的性质. 因此环 $\mathbb{Z}_m$ 既可看作模 m 的剩余类集，也可看作这些类的代表元集.

4. 环的类型. 域 在我们熟知的数环 $\mathbb{Z}, \mathbb{Q}$ 和 $\mathbb{R}$ 中，从 $ab = 0$ 可得 $a = 0$ 或 $b = 0$. 但在任何上述环上的方阵环中，却没有这个性质. 利用矩阵 E_{ij}(见第 2 章 §3 定理 4 的证明), 当 $j \neq k$ 时，我们有等式 $E_{ij}E_{ki} = 0$, 尽管 $E_{ij} \neq 0$, 且 $E_{ki} \neq 0$. 我们指出 $E_{ik}E_{kj} = E_{ij} \neq 0$. 人们可能会认为，如此不正常是由于环 M_n 的非交换性，但

事实并非如此. 我们在第 2 段中已经看到, 在交换环 $\mathbb{Z}_4$ 中有等式 $2 \odot 2 = 0$, 与人所共知的真理 "2 乘以 2 等于 4" 相违背. 再给出两个例子.

例 5 数对 (a, b)(此处可设 a, b 取自 $\mathbb{Z}, \mathbb{Q}$ 或 $\mathbb{R}$), 连同如下定义的加法和乘法显然构成一个环:

$$(a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2),$$

$$(a_1, b_1) \cdot (a_2, b_2) = (a_1 a_2, b_1 b_2),$$

这个环是交换的, 带有单位元 (1,1). 我们再次遇到了同样的现象: $(1,0) \cdot (0, 1) = (0,0) = 0$.

例 6 在实函数环 $\mathbb{R}^{\mathbb{R}}$ 中 (见第 1 段的例 3), 函数 $f : x \mapsto |x| + x$ 和 $g : x \mapsto |x| - x$ 具有这样的性质: 当 $x \leqslant 0$ 时, $f(x) = 0$, 而当 $x \geqslant 0$ 时 $g(x) = 0$. 所以它们的逐点乘积 fg 是零函数, 尽管 $f \neq 0$ 且 $g \neq 0$.

定义 在环 R 中, 如果 $a \neq 0, b \neq 0$, 但 $ab = 0$, 则 a 叫作 **左零因子**, 而 b 叫作 **右零因子**(在交换环 R 中简称为 零因子). 在非零环 R 中, 零本身叫作 平凡零因子. 如果环 R 除 0 外没有其他的零因子, 则 R 叫作 **无零因子环**. 如果一个交换环 R 含有 $1 \neq 0$, 并且无零因子, 则称 R 为 **整环**(**整性环** 或 **具有整性**).

定理 1 有单位元的非平凡交换环 R 是整环, 当且仅当在 R 中 消去律 成立, 即对任意 $a, b, c \in R$,

$$ab = ac, \quad a \neq 0 \Rightarrow b = c.$$

证明 若在 R 中有消去律, 那么从 $ab = 0 = a \cdot 0$ 推出或者 $a = 0$, 或者 $a \neq 0$ 但 $b = 0$. 反之: 如果 R 是整环, 则

$$ab = ac, a \neq 0 \Rightarrow a(b - c) = 0 \Rightarrow b - c = 0 \Rightarrow b = c. \qquad \square$$

在有单位元的环 R 中自然要考察可逆元素的集合. 元素 a 称为 **可逆的**(或 **单位**), 若存在元素 a^{-1}, 使得 $aa^{-1} = 1 = a^{-1}a$. 准确地说, 应该谈元素是 **右可逆的** 或 **左可逆的**(它们分别指存在元素 b, 使 $ab = 1$ 或 $ba = 1$), 但在交换环或无零因子环中, 这两个概念是一致的. 事实上, 在无零因子环中从 $ab = 1$ 得到 $aba = a, a(ba - 1) = 0$, 由于 $a \neq 0$, 故 $ba - 1 = 0$, 即 $ba = 1$.

我们知道, 例如, 在环 M_n 中, 可逆元素恰为行列式不为零的矩阵. 一个可逆元素 a 不可能是零因子:

$$ab = 0 \Rightarrow a^{-1}(ab) = 0 \Rightarrow (a^{-1}a)b = 0 \Rightarrow 1 \cdot b = 0 \Rightarrow b = 0$$

(类似地, $ba = 0 \Rightarrow b = 0$). 所以毫不奇怪, 成立如下的

定理 2 设 R 是有单位元的环, 则环 R 中的全体可逆元素构成一个乘法群 $U(R)$.

证明　事实上，$U(R)$ 包含单位元，$a \in U(R) \Rightarrow a^{-1} \in U(R)$, 且 R 中的乘法满足结合律，因而我们只需验证 $U(R)$ 对于乘法封闭，即从 $U(R)$ 中任取两个元素 a 和 b, 乘积 ab 也在 $U(R)$ 中. 但这是显然的，因为

$$(ab)^{-1} = b^{-1}a^{-1} \quad (ab \cdot b^{-1}a^{-1} = a(bb^{-1})a^{-1} = a \cdot 1 \cdot a^{-1} = aa^{-1} = 1),$$

表明 ab 是可逆的. □

不难看到，$U(\mathbb{Z}) = \{\pm 1\}$ 是一个 2 阶循环群.

如果将环的定义中的公理 R2) 换成更强的条件，我们可以得到一类非常有趣的环称为 **除环** 或 **斜域**.

R2′) $R^* = R \backslash \{0\}$ 关于乘法运算构成一个群.

除环永远没有零因子，其中的每一个非零元素都可逆，在交换除环中，加法和乘法运算几乎是完全对称的，这种环叫作 **域**.

我们再次强调

定义　*设 P 是一个有单位元 $1 \neq 0$ 的交换环，如果 P 的每一个非零元素都可逆，则称 P 为一个* **域**. *群 $P^* = U(P)$ 叫作* **域的乘法群**.

域是自身的两个阿贝尔群，加法群和乘法群的混合物，它们用分配律联系在一起 (现在由于交换性，只用一个分配律就够了).

乘积 ab^{-1} 一般写成 **分式** 的形式 $\frac{a}{b}$(或 **比例式**, **商**), 为了节省篇幅，有时借助斜线写成 a/b. 分式 a/b 仅当 $b \neq 0$ 时有意义，它是方程 $bx = a$ 的唯一解.

分式的运算遵循下述法则：

$$\begin{aligned}
&\frac{a}{b} = \frac{c}{d} \Leftrightarrow ad = bc, \quad b,\ d \neq 0,\\
&\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}, \quad b,\ d \neq 0,\\
&-\frac{a}{b} = \frac{-a}{b} = \frac{a}{-b}, \quad b \neq 0,\\
&\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}, \quad b,\ d \neq 0,\\
&\left(\frac{a}{b}\right)^{-1} = \frac{b}{a}, \quad a, b \neq 0.
\end{aligned} \tag{8}$$

这是在中学就已经知道的通常的法则，但我们不仅需要记住它，也要从域的公理出发推导它，这样做并不困难. 我们来看一下法则 (8) 中第二个式子的推导就足够了. 设 $x = a/b$, 且 $y = c/d$ 分别是方程 $bx = a$ 和 $dy = c$ 的解. 从这两个方程得到

$$dbx = da, bdy = bc \Rightarrow bd(x + y) = da + bc \Rightarrow t = x + y = \frac{da + bc}{bd}$$

是方程 $bdt = da + bc$ 的唯一解.

如果域 P 中的子环 F 自身也是一个域，则称 F 为 P 的 **子域**. 例如有理数域 $\mathbb{Q}$ 是实数域 $\mathbb{R}$ 的子域.

当域 $F\subset P$ 时，我们也称 P 是 F 的一个 **扩域**. 由子域的定义易见，域 P 的零元和单位元属于 F, 并且也是 F 的零元和单位元. 若某元素 $a\in P$, 但 $a\notin F$, 取域 P 中包含有 F 和元素 a 的所有子域的交 F_1, 则 F_1 是包含有集合 $\{F,a\}$ 最小的子域 (论证与群的情况类似，见 §2 习题 1).

我们称 F_1 是由域 F 添加元素 a 得到的扩域，记作 $F_1=F(a)$. 类似地，域 P 的子域 $F_1=F(a_1,\cdots,a_n)$ 是由 F 添加 n 个元素 $a_1,\cdots,a_n$ 得到的.

易见 $\mathbb{Q}(\sqrt{2})$ 由形如 $a+b\sqrt{2}$ 的数组成，此处 $a,b\in\mathbb{Q}$, 这是因为 $(\sqrt{2})^2=2$, 当 $a+b\sqrt{2}\neq 0$ 时， $\dfrac{1}{a+b\sqrt{2}}=\dfrac{a}{a^2-2b^2}-\dfrac{b}{a^2-2b^2}\sqrt{2}$. 对于域 $\mathbb{Q}(\sqrt{3}),\mathbb{Q}(\sqrt{5})$ 等等有类似的结果.

域 P 与 P' 称为 **同构的**, 若它们作为环是同构的. 根据定义，对于任意同构映射 $f,f(0)=0'$, $f(1)=1'$. 谈域的同态意义不大，因为

$$\begin{aligned}\ker f\neq 0\Rightarrow f(a)=0,a\neq 0\Rightarrow f(1)=f(aa^{-1})=f(a)f(a^{-1})=0\cdot f(a^{-1})=0\\ \Rightarrow\forall b,\ \ f(b)=f(1\cdot b)=f(1)f(b)=0\cdot f(b)=0\Rightarrow\ker f=P.\end{aligned}$$

但是，域的 **自同构**, 即域 P 到自身的同构映射与域的最本质的性质紧密相联，也是在伽罗瓦理论中研究这些本质性质的强有力的工具.

域扩张的概念源自人类扩大数的范围的愿望. 这一漫长的历史过程可以粗略地体现在下图中：

$$\begin{aligned}\{1\}\rightsquigarrow\{1+1=2\}\rightsquigarrow\mathbb{N}\rightsquigarrow\{\mathbb{N},0\}\rightsquigarrow\\ \rightsquigarrow\mathbb{Z}\rightsquigarrow\mathbb{Q}\rightsquigarrow\mathbb{Q}(\sqrt{2})\rightsquigarrow\mathbb{R}\end{aligned}$$

这个过程延续至今，形成了分支众多的域系，已经远离了人们所熟悉的通常的数系. 在这一过程中，并非每个阶段都是纯代数的. 例如从有理数过渡到实数时，使用了连续性和完备性的概念 (柯西序列极限的存在性), 这件事已在数学分析课程中讲过了. 用完全类似的方法可以构造 p-adic 数域，我们在这里不对它展开讨论，在此基础上引出的现代 p-adic 分析是数学的三个分支：数论、代数和分析的杰出产物.

5. 域的特征 我们在第 2 段中构造了有限剩余类环 $\mathbb{Z}_m$, 其元素为

$$\bar{0},\ \bar{1},\ \bar{2},\ \cdots,\ \overline{m-1},$$

加法运算是 $\bar{k}+\bar{l}=\overline{k+l}$, 乘法运算是 $\bar{k}\cdot\bar{l}=\overline{kl}$(我们不再使用符号 $\oplus$ 和 $\odot$). 如果 $m=st$, $s>1$,$t>1$, 则 $\bar{s}\cdot\bar{t}=\bar{m}=\bar{0}$, 即 $\bar{s}$ 和 $\bar{t}$ 是 $\mathbb{Z}_m$ 中的零因子.

现在设 $m=p$ 是一个素数. 我们断言， $\mathbb{Z}_p$ 是一个域 (它包含 p 个元素). 当 $p=2,3$ 时，从第 2 段中的乘法表可直接看出这一点. 在一般情况下，只要对任意 $\bar{s}\in\mathbb{Z}_p^*$, 指出逆元 $\bar{s}'$ 的存在性就可以了 (整数 s 和 s' 显然不能被 p 整除).

考察元素

$$\bar{s}, \overline{2s}, \cdots, \overline{(p-1)s}. \tag{9}$$

它们都不等于零，这是因为当 $k=1,2,\cdots,p-1$ 时

$$s \not\equiv 0(\bmod p) \Rightarrow ks \not\equiv 0 \pmod p,$$

这里用到了 p 是素数. 同理可证，(9) 式中的元素两两不等：若 $k<l$, 而 $\overline{ks}=\overline{ls}$, 则 $\overline{(l-k)s}=\bar{0}$, 这是不可能的. 于是除了排列的顺序，(9) 式中元素的序列与序列

$$\bar{1}, \bar{2}, \cdots, \overline{p-1}$$

重合. 特别地，可以找到整数 $s', 1 \leqslant s' \leqslant p-1$, 使得 $\overline{s's}=\bar{1}$. 这就表明 $\overline{s'}\bar{s}=\bar{1}$, 即 $\overline{s'}$ 是 $\bar{s}$ 的逆元. 这样我们就证明了下述的

定理 3　剩余类环 $\mathbb{Z}_m$ 是一个域，当且仅当 $m=p$ 是一个素数.

推论(费马小定理)　设 p 是素数，m 是一个不能被 p 整除的整数，则有同余式

$$m^{p-1} \equiv 1(\bmod p).$$

证明　我们已经看到，两个集合

$$\{\bar{m}, \bar{2}\bar{m}, \cdots, (\overline{p-1})\bar{m}\} = \{\bar{1}, \bar{2}, \cdots, \overline{p-1}\}.$$

(在 (9) 式中将 s 换成 m, 并注意到等式 $\overline{km}=\bar{k}\bar{m}$, $k=1,\cdots,p-1$). 将左右两个集合的全体元素分别连乘，我们得到

$$\left(\prod_{k=1}^{p-1} \bar{k}\right) \bar{m}^{p-1} = \prod_{k=1}^{p-1} \bar{k}.$$

因为 $\mathbb{Z}_p$ 是无零因子环，根据定理 1, 乘积 $\prod_{k=1}^{p-1} \bar{k} \neq 0$, 故可约去，得到 $\bar{m}^{p-1} \equiv \bar{1}$. 换成同余的语言，即得到所需的式子. □

比费马小定理更一般的欧拉定理成立，但该定理的必要性只有在 [BAIII] 中给出.

尽管域 $\mathbb{Z}_2, \mathbb{Z}_3, \mathbb{Z}_5, \cdots$ 与我们已知的域 $\mathbb{Q}, \mathbb{Q}(\sqrt{2}), \mathbb{R}$ 如此不同，但它们在域论中占据的地位与我们熟知的 $\mathbb{Q}$ 的相应地位是一致的. 这件事可作如下说明. 设 P 是域.

我们已经知道任取子域族 $\{P_i | i \in I\}$, 其交集 $\bigcap_i P_i$ 仍是 P 的子域.

定义　一个域如果不包含任意真子域，则称之为**素域**.

定理 4　任意一个域 P 包含且仅包含一个素域 P_0.P_0 同构于 $\mathbb{Q}$ 或 $\mathbb{Z}_p$, 其中 p 是一个素数.

证明 假设存在两个不同的素域 $P', P'' \subset P$, 则它们的交 $P' \cap P''$ 是不同于 P' 和 P'' 的一个域 (交是非空的，因为 0 和 1 既包含在 P' 中，也包含在 P'' 中). 根据 P' 和 P'' 的素性，这是不可能的. 因而素域 $P_0 \subset P$ 如果存在，必须是唯一的.

域 P 中包含有元素 1 以及 1 的任意倍数 $n \cdot 1 = 1 + 1 + \cdots + 1$. 根据在一个环中元素的加法与乘法的运算性质 (见第 1 段最后),

$$s \cdot 1 + t \cdot 1 = (s + t) \cdot 1, (s \cdot 1)(t \cdot 1) = (st) \cdot 1; s, t \in \mathbb{Z}.$$

我们来定义一个映射 $f: \mathbb{Z} \to P$, 由 $f(n) = n \cdot 1$ 给出，易见 f 是一个同态，其核为 $\ker f = m\mathbb{Z}$, 如果 m=0, 则 f 是单同态，分式 $(s \cdot 1)/(t \cdot 1), s, t \in \mathbb{Z}, t \neq 0$, 在 P 中有意义 (因为 P 是域), 它们组成与 $\mathbb{Q}$ 同构的域 P_0. 即为 P 的素子域.

如果 $m > 0$, 那么显然如下定义的映射

$$f^*: \bar{k} = \{k\}_m \mapsto f(k)$$

是一个嵌入 $\mathbb{Z}_m \to P$. 根据定理 3, 当且仅当 $m = p$ 为素数时才有可能. 这时 $f^*(\mathbb{Z}_p)$ 是 P 的素子域. □

定义 称域 P 有特征零，若 P 的素子域 P_0 同构于 $\mathbb{Q}$; 称域 P 有素 (或有限) 特征 p, 若 $P_0 \simeq \mathbb{Z}_p$. 分别记作 $\mathrm{char} P = 0$ 或 $\mathrm{char} P = p > 0$.

通常用 $\mathbb{F}_p$ 或 GF(p)(伽罗瓦域) 作为 p 元 “抽象” 域的符号代替 $\mathbb{Z}_p$. 令 p 是素数， n 是任意正整数， $q = p^n$, 存在 q 元有限域 GF(q). 我们将在 [BAⅢ] 中回到这个有趣的问题上来，现在仅给出一个例子，描述带有 4 个元素 $\{0, 1, \alpha, \beta\}$ 的域:

GF(4):

$+$	0	1	α	β
0	0	1	α	β
1	1	0	β	α
α	α	β	0	1
β	β	α	1	0

$\cdot$	0	1	α	β
0	0	0	0	0
1	0	1	α	β
α	0	α	β	1
β	0	β	1	α

α 和 β 是什么并不重要. 读者不妨自行验证加法和乘法满足分配律.

特征零表明在域 P 的加法群中，元素 1 的阶是**无限的**. 类似地，有限特征 p 表明，在域 P 的加法群中，任意非零元素的阶是 p:

$$px = x + \cdots + x = 1 \cdot x + \cdots + 1 \cdot x = (1 + \cdots + 1) \cdot x = (p \cdot 1)x = 0.$$

6. 关于线性方程组的注记 现在将目光转向前几章的线性方程组和行列式理论. 我们讨论过的线性方程组的系数和矩阵中的元素是数 (有理数或实数), 但并未用到这些数的特性. 因而用指定域 P 中的元素代替数不会有任何障碍. 这时结果应当用域 P 的术语来阐述：线性方程组解的分量和函数 det 的值均在 P 中. 解线性方程组的高斯算法，行列式理论，克拉默法则对任意域 P 仍然有效 (即没有变化).

例 7　设给定一个齐次线性方程组 $AX = 0$, 系数矩阵为

$$A = (a_{ij}) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ -10 & 13 & 14 & 15 \\ 12 & -9 & 14 & 15 \\ 12 & 13 & -8 & 15 \end{pmatrix}$$

未知数所成的列向量为 $X = [x_1, x_2, x_3, x_4]$, 直接计算可得 $\det A = 2^3 \cdot 11^3$. 从而令 P 是任意特征零或特征 $p \neq 2,11$ 的域 (这时整数 $1, 2, 3, 4, -10, \cdots, 15$ 可由相应的剩余类代替), a_{ij}, $x_k \in P$, 则方程组是确定的, 仅有唯一的平凡解 $X = 0$.

如果 $\mathrm{char}\, P = 2$(例如 $P = \mathbb{Z}_2$), 那么根据同余式

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ -10 & 13 & 14 & 15 \\ 12 & -9 & 14 & 15 \\ 12 & 13 & -8 & 15 \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix} \pmod 2$$

我们得知系数矩阵的秩为 2, 方程组有两个线性无关的解 $X_1 = [1, 0, 1, 0], X_2 = [0, 1, 0, 1]$. 为避免混淆, 本应写成 $X_1 = [\bar{1}, \bar{0}, \bar{1}, \bar{0}], X_2 = [\bar{0}, \bar{1}, \bar{0}, \bar{1}]$, 但是我们已经有充分的准备去领会简化的记法.

如果 $\mathrm{char}\, P = 11$, 则由同余式

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ -10 & 13 & 14 & 15 \\ 12 & -9 & 14 & 15 \\ 12 & 13 & -8 & 15 \end{pmatrix} \equiv \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} \pmod{11}$$

得到, 方程组有 3 个线性无关的解

$$X_1 = [9, 1, 0, 0], \quad X_2 = [8, 0, 1, 0], \quad X_3 = [7, 0, 0, 1].$$

正如我们已经看到的那样, 方程组解的个数依赖于域 P, 但解方程组的过程与平常没有任何不同. 从 $\mathbb{Q}$ 和 $\mathbb{R}$ 过渡到一般域的好处之一是避免了论述中的重复. 但还有更重要的原因.

直到现在当我们谈到一般线性群时, 总是指系数取自 $\mathbb{Q}$ 或 $\mathbb{R}$ 的全体非退化矩阵组成的群. 系数取自域 P 的 n 阶方阵的全体构成矩阵环 $M_n(P)$, 而所有非退化矩阵 $A \in M_n(P)$($\det A \neq 0$ 的矩阵) 构成域 P 上的一般线性群 $\mathrm{GL}_n(P)$. 改变域 P, 例如取 $P = F_p$, 就可以自然地得到一系列重要的群 (见 [BAⅢ]).

形如 $\mathbb{R}, \mathbb{Q}, \mathbb{Q}(\sqrt{2})$ 的域通常称为 **数域**. 域 $\mathbb{F}_p$ 是一个非数域的例子: 不正规地称其元素为数, 仅仅基于这些元素可与整数集 $\{0, 1, \cdots, p-1\}$ 等同看待.

在第 1 章 §2 中我们提到过有限域在编码理论中的应用 (问题 3). 现在给出这个课题的一个小例子.

例 8 为了传送 $PEACE$ 一词, 原则上利用四个基本信息单元

$$P=(0,0),\quad E=(1,0),\quad A=(0,1),\quad C=(1,1)$$

就够了, 我们的译码可看作二元域 $\mathbb{F}_2\cong\mathbb{Z}_2=\{0,1\}$ 上的二维向量空间 $\mathbb{F}_2^2$ 的行向量. 但是在传送过程中, 可能发生干扰 (将 0 变为 1 或 1 变为 0), 结果终端得到的可能是, 例如 $APACE$, 根据 香农(Shannon)的基本定理, 增加基本信息单元的长度 (即增加传送的行向量的长度) 可以清除干扰. 假设根据传送条件知道, 在每个长为 5 的基本信息单元中最多出现一个失真. 那么在向量空间 $S=\mathbb{F}_2^5$ 中取子集

$$S_0=\{P=(0,0,1,1,0),\quad E=(1,0,0,1,1),\quad A=(0,1,1,0,1),\\ C=(1,1,0,0,0)\},$$

称之为 **编码向量**.

编码向量	00110	10011	01101	11000
编码向量失真后得到的向量	00010 00100 00111 01110 10110	00011 10001 10010 10111 11011	00101 01001 01100 01111 11101	01000 10000 11100 11001 11010

从表中可以看到, 不同列中的失真向量的集合交为空, 因此正确的结果是可能得到的, 也就是说, 可以恢复真实的信息.

我们得到了 *可以纠正一个错误的编码* S_0, 对于充分大的维数 n, 利用向量空间 $\mathbb{F}_2^n$, 可以构造类似的编码, 没有错误地传送所有的字母, 从而准确地传送任何文章, 为了避免过长和过于缓慢的译码, S_0 要经过专门的选择. 有许多办法可以做到这一点, 其中包括利用有限域 $\mathbb{F}_q$ 的纯代数方法.

习 题

1. 拓展 §1 例 2 的想法, 证明集合 $\mathcal{P}(\Omega)$ 在运算

$$A+B=(A\cup B)\backslash(A\cap B), AB=A\cap B, A,B\in\Omega$$

之下是一个有单位元的环, 其加法群的元素阶为 2.

2. 如果环中的任意元素 x 满足方程 $x^2=x$, 证明该环是交换环. 若条件改为 $x^3=x$, 结论还成立吗?

3. 域 $\mathbb{Q}(\sqrt{2})$ 和 $\mathbb{Q}(\sqrt{5})$ 同构吗?

4. 证明交换环的满同态像仍是交换环.

5. 证明任意有限整环 R 是一个域.

6. 设 p 是素数， R 是有单位元的交换环，使得任取 $x \in R, px = 0$. 证明

$$(x+y)^{p^m} = x^{p^m} + y^{p^m}, \quad m = 1, 2, \cdots.$$

提示：对 m 作归纳，注意到二项系数 $\begin{pmatrix} p \\ k \end{pmatrix}$ 当 $0 < k < p$ 时被 p 整除.

7. 证明含有 5 个元素的环或同构于 $\mathbb{Z}_5$, 或是带有零乘法的环.

8. 环 R 的非零元素 x 称为**幂零的**, 若存在 $n \in \mathbb{N}$, 使得 $x^n = 0$. 证明:

1) 若 R 是任意有单位元的环， x 是幂零元，则 $1 - x$ 是可逆元;

2) 环 $\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z}$ 包含有幂零元，当且仅当 m 可以被一个大于 1 的整数的平方整除.

9. 若环 R 有单位元，且基数 $|R|$ 是无限的，则非零不可逆元素的个数不可能是一个有限整数.

提示： 用反证法. 设 $N = \{a_1, \cdots, a_n\}$ 是环 R 中所有的非 0 不可逆元素的集合. 对任意 $x \in R \backslash (N \cup \{0\})$, 映射 $\rho_x : a_i \mapsto xa_i$ 是 $N \to N$ 的一个双射映射 $\rho : x \mapsto \rho_x$ 的核 $\ker \rho$ 是无限的.

10. 设 R 是任意有单位元 1 的结合环， a, b 是 R 的元素. 证明

$$(1 - ab)c = 1 = c(1 - ab) \Rightarrow (1 - ba)d = 1 = d(1 - ba),$$

其中 $d = 1 + bca$, 即 $1 - ab$ 在 R 中可逆意味着 $1 - ba$ 也可逆. 元素 $1 + adb$ 等于什么?

11. 证明矩阵 $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$, 其中 $a, b \in \mathbb{Z}_3$, 构成一个 9 元域，而这个域的乘法群是 8 阶循环群.

12. 在本节最后的例 2 中构造的编码 S_0 能否纠正两个错误?

第 5 章　复数和多项式

在本章中将考察一些非常具体的代数系统，虽然我们在初等数学中已对它们有所了解，但仍然值得在这里作进一步的研究．上一章的观点使我们对早期传统的代数领域产生了新的看法．与此同时，多项式的例子使环的扩张以及在整环 (整区) 中因子分解的唯一性更好理解且更易于把握．

§1　复数域

数学史表明，“虚”数的拥护者和反对者之间曾进行过长期的争论，该数来自代数方程

$$x^2+1=0. \tag{1}$$

可以简单地约定将方程 (1) 的解形式地记作 $\pm\sqrt{-1}$, 但更深远的问题是，赋予这一记法以某种意义．我们将在不同的层次上解决这一问题．先提出几个富有启发性的设想．

1．辅助结构　我们希望将实数域 $\mathbb{R}$ 进行扩张，使得方程 (1) 在新的域中有解．形如

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \in M_2(\mathbb{R}) \tag{2}$$

的全体二阶方阵的集合 P 可作为这种扩张的一个模型．我们断言，P 是一个域 (比较第 4 章 §3 习题 11).

事实上，P 包含有环 $M_2(\mathbb{R})$ 的零元 (零矩阵) 和单位元 (单位矩阵 E). 其次，

从关系式

$$
\begin{pmatrix} a & b \\ -b & a \end{pmatrix} + \begin{pmatrix} c & d \\ -d & c \end{pmatrix} = \begin{pmatrix} a+c & b+d \\ -(b+d) & a+c \end{pmatrix},
$$

$$
-\begin{pmatrix} a & b \\ -b & a \end{pmatrix} = \begin{pmatrix} -a & -b \\ -(-b) & -a \end{pmatrix}, \tag{3}
$$

$$
\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \begin{pmatrix} c & d \\ -d & c \end{pmatrix} = \begin{pmatrix} ac-bd & ad+bc \\ -(ad+bc) & ac-bd \end{pmatrix}
$$

得到, P 关于加法和乘法运算封闭. 这两种运算的结合性是它们在 $M_2(\mathbb{R})$ 中结合性的推论. 分配律和加法的交换性可同样得到. 这样 P 是 $M_2(\mathbb{R})$ 的一个子环. P 中乘法的交换性由公式 (3) 的 3 式保证, 最后只需证明若 P 中任意形如 (2) 的矩阵带有非零行列式 $a^2+b^2 \neq 0$, 则在 P 中有逆矩阵.

可以利用求逆矩阵的公式 (见第 3 章 §3 定理 1) 直接计算, 也可以根据条件

$$
\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \begin{pmatrix} x & y \\ -y & x \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}
$$

列出线性方程组

$$
ax - by = 1,
$$

$$
bx + ay = 0,
$$

求解后得到

$$
\begin{pmatrix} a & b \\ -b & a \end{pmatrix}^{-1} = \begin{pmatrix} c & d \\ -d & c \end{pmatrix}, \tag{4}
$$

其中 $c = \dfrac{a}{a^2+b^2}, d = \dfrac{-b}{a^2+b^2}$.

运用第 2 章 §3 数与矩阵相乘的公式 (5), 我们将域 P 的任意元素写成如下形式:

$$
\begin{pmatrix} a & b \\ -b & a \end{pmatrix} = aE + bJ, \quad a, b \in \mathbb{R}, \quad J = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}. \tag{5}
$$

域 P 包含有子域 $\{aE | a \in \mathbb{R}\} \cong \mathbb{R}$, 而关系式

$$
J^2 + E = 0
$$

指出, 元素 $J \in P$"精确到同构" 是方程 (1) 的解, 因而此处无需神秘地将 J 当作 "虚构的量".

但称为复数域的并不是域 P, 而是一个同构于 P, 其元素等同于平面上的点的域. 希望域 P 有几何实现不是偶然的, 在我们的心目中实数域 $\mathbb{R}$ 与 "实直线" 密不可分, 实直线上有一个定点表示 0, 并有一个单位长度用于确定 1 的位置.

2. 复平面 于是, 我们希望构造一个域 $\mathbb{C}$, 其元素是实平面 $\mathbb{R}^2$ 上的点, 点的加法和乘法满足域的运算律, 并使方程 (1) 在其中可解. 取笛卡儿平面上的直角坐标系, x 轴是横轴, y 轴是纵轴. 记 (a,b) 为横坐标为 a, 纵坐标为 b 的点. 任取点 $(a,b),(c,d)$ 如下定义它们的和与积

$$\begin{aligned}(a,b)+(c,d)&=(a+c,b+d),\\(a,b)(c,d)&=(ac-bd,ad+bc)\end{aligned}\tag{6}$$

(仍然用实数域 $\mathbb{R}$ 中的记号 $+,\cdot$, 应该不至引起混淆). 直接但乏味的验证使我们确信, 给定的运算使有序数对 (平面上的点) 的集合构成了一个域. 幸运的是, 我们无需做这样的验证. 将平面 $\mathbb{C}$ 上的点对应到前面构造的域 P 的元素

$$(a,b)\mapsto\begin{pmatrix}a & b\\ -b & a\end{pmatrix},$$

公式 (3) 和 (6) 确保我们得到了一个同构, 从而集合 $\mathbb{C}$ 是一个域. 通常称之为 **复数域**. 由于该域的几何实现, $\mathbb{C}$ 也叫作 **复数平面**(更经常地叫作 **复平面**).

横轴, 即点 $(a,0)$ 的集合与实直线有相同的性质, 可设 $(a,0)=a$. 域的零元 (0,0) 和单位元 (1,0) 与通常实数的零元和单位元一致. 纵轴上的点 (0,1) 自欧拉和高斯的时代起便记作 i, 称之为 "虚数单位", 它是方程 (1) 的根: $i^2=(0,1)(0,1)=(-1,0)=-1$. 任意复数 $z=(x,y)=(x,0)+(0,1)(y,0)$ 现在可以用通常的方式写成

$$z=x+iy,\quad x,y\in\mathbb{R}\tag{7}$$

这个写法十分接近域 P 元素的表达式 (5). 注意到 $\mathbb{Q}\subset\mathbb{R}\subset\mathbb{C}$. 所以 $\mathbb{C}$ 是一个特征为零的域 (见第 4 章 §3 第 5 段).

3. 复数运算的几何解释 复平面 $\mathbb{C}$ 的横轴通常叫作 **实轴**, 纵轴叫作 **虚轴**, 虚轴上的数 iy 叫作 **纯虚数**, 尽管 "虚" 这个词已经失去了它原有的含义. 在写法 (7) 中, x 叫作复数 z 的 **实部**, 记作 $\mathrm{Re}z$, 而 y 叫作 z 的 **虚部**, 记作 $\mathrm{Im}z$. 将任意复数 $z=x+iy$ 对应到共轭复数 $\bar{z}=x-iy$ 的映射叫作 **复共轭映射**. 在几何上, 它对应于复平面沿实轴的反射 (图 18).

一个值得注意的重要事实是

定理 1 *映射 $z\mapsto\bar{z}$ 是域 $\mathbb{C}$ 的 2 阶自同构, 使得所有的实数保持不变. 任意复数与它的共轭复数的和与积是实数.*

证明 根据共轭复数的定义, 若 $x\in\mathbb{R}$, 则 $\bar{x}=x$. 特别地, $\bar{0}=0,\bar{1}=1$. 复共轭映射以 2 为阶的结论也是显然的: $\overline{(\bar{z})}=z$. 我们还需要验证关系式

$$\overline{z_1+z_2}=\bar{z}_1+\bar{z}_2,\overline{z_1z_2}=\bar{z}_1\bar{z}_2,\tag{8}$$

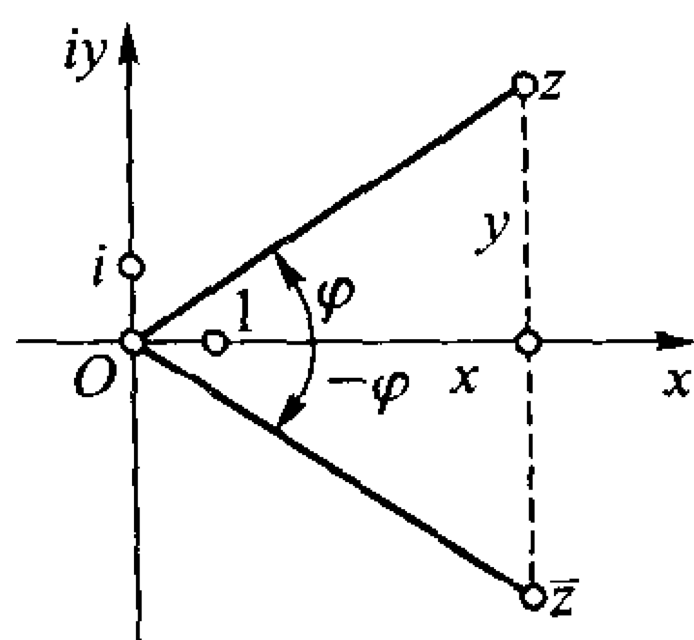


图 18

它们可直接从公式 (6) 得到，只要把 (6) 式改写成下述形式即可：

$$\begin{aligned}(x_1+iy_1)+(x_2+iy_2)&=(x_1+x_2)+i(y_1+y_2),\\(x_1+iy_1)\cdot(x_2+iy_2)&=(x_1x_2-y_1y_2)+i(x_1y_2+x_2y_1).\end{aligned}\tag{9}$$

数 $z=x+iy$ 与其共轭复数 $\bar{z}=x-iy$ 的和与积是公式 (9) 的特殊情况：$z+\bar{z}=2x$, $z\bar{z}=x^2+y^2$. □

注记　在复数域 $\mathbb{C}$ 的诸多自同构中，复共轭是唯一的连续自同构 (即将复平面 $\mathbb{C}$ 上点的邻域仍变为邻域). 我们不给出这一论断的精确表述和证明.

复数 $z=x+iy$ 的模是非负实数 $|z|=\sqrt{z\bar{z}}=\sqrt{x^2+y^2}$. 如所周知，点 z 在平面上的位置由它的极坐标完全确定：即从坐标原点到 z 点的距离 $r=|z|$, 以及横轴的正方向与坐标原点到 z 的正方向之间的夹角 φ(见图 18). 角 φ 叫作 z 的 **辐角**, 记作 $\arg z=\varphi$. 根据定义， $\arg z$ 可以取任意的正值和负值，但对于给定的 r, 相差 2π 的整倍数的辐角都对应于同一个数. 数 0 的模是 $|0|=0$, 但 0 的辐角没有定义.

对于复数而言， "大于" 和 "小于" 关系没有意义，即它们之间不能用不等号连接：与实数不同，实数的辐角仅有两个主值，即 0(正实数) 和 π(负实数),*而复数不是有序的*.

准确地说，在 $\mathbb{C}$ 中不存在满足如下性质的 $>$ 关系：

i) 如果 $z\in\mathbb{C}$, 则 $z>0$,$z=0$ 或 $-z>0$;

ii) 从 $u>0$,$v>0$ 可得 $u+v>0$ 和 $u\cdot v>0$.

事实上，假设由 $z\neq 0$ 可得 $z^2>0$(如同在实数域 $\mathbb{R}$ 中). 则有 $1^2>0$, $i^2>0$, 并根据 ii), $0=i^2+1>0$, 得到矛盾.

极坐标 r 和 φ 可以通过下述著名的公式确定 x 和 y

$$x=r\cos\varphi,\quad y=r\sin\varphi,\quad z=r(\cos\varphi+i\sin\varphi).\tag{10}$$

它叫作 **复数 z 的三角形式**.

复数 z 与 z' 的和可以在笛卡儿坐标系中利用平行四边形法则简单地得到，或等价地说成，从坐标原点出发分别对应于数 z, z' 的有向线段 (向量) 相加的法则 (见

图 19). 在图 19 中比较以点 0,z 和 $z+z'$ 为顶点的三角形的三条边 (它们等同于对应的复数的模), 我们得到了重要的不等式.

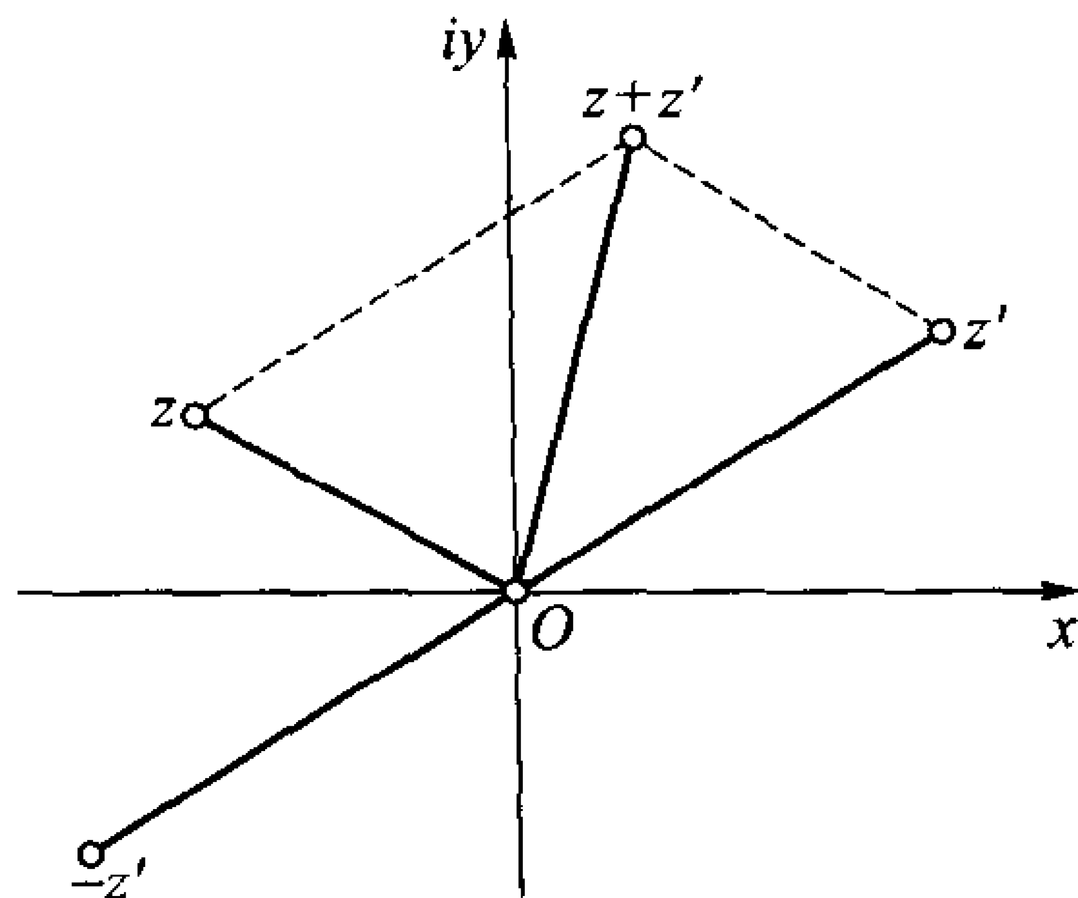


图 19

$$|z+z'| \leqslant |z| + |z'|. \tag{11}$$

我们指出, 不等式 (11) 可以写成更一般的形式

$$|z| - |z'| \leqslant |z \pm z'| \leqslant |z| + |z'|,$$

与实数域中相应的不等式完全类似.

复数的乘法可由极坐标方便地表示出来.

定理 2 复数 z, z' 的乘积的模等于因子模的乘积, 而辐角等于因子的辐角之和:

$$|zz'| = |z| \cdot |z'|, \quad \arg\, zz' = \arg\, z + \arg\, z'. \tag{12}$$

类似地,

$$\left|\frac{z}{z'}\right| = \frac{|z|}{|z'|}, \quad \arg \frac{z}{z'} = \arg\, z - \arg\, z'.$$

证明 事实上, 设 z 和 z' 的三角形式为

$$z = r(\cos\varphi + i\sin\varphi), \quad z' = r'(\cos\varphi' + i\sin\varphi').$$

直接相乘或利用 (9) 式得到

$$zz' = rr'\left[(\cos\varphi\cos\varphi' - \sin\varphi\sin\varphi') + i(\cos\varphi\sin\varphi' + \sin\varphi\cos\varphi')\right],$$

根据众所周知的三角公式, 这就是复数 zz' 的三角形式:

$$zz' = |z| \cdot |z'| \left[\cos(\varphi+\varphi') + i\sin(\varphi+\varphi')\right].$$

其次, 若 $z'' = z/z'$, 则 $z = z'z''$. 因而对乘积 $z'z''$ 应用已证明的公式 (12), 我们就得到了关于分式 z/z' 的公式. □

特别地,

$$z^{-1} = |z|^{-1}\left[\cos(-\varphi) + i\sin(-\varphi)\right].$$

为了在复平面上得到 z^{-1}(图 20), 需要对 z 做关于单位圆的反演, 得到点 z'("反演"指 z' 到点 O 的距离是 z 到点 O 距离的倒数), 然后做关于实轴的反射 (或由 $z' \mapsto \overline{z'}$ 给出的自同构), 则 z' 的像即为 z^{-1}.

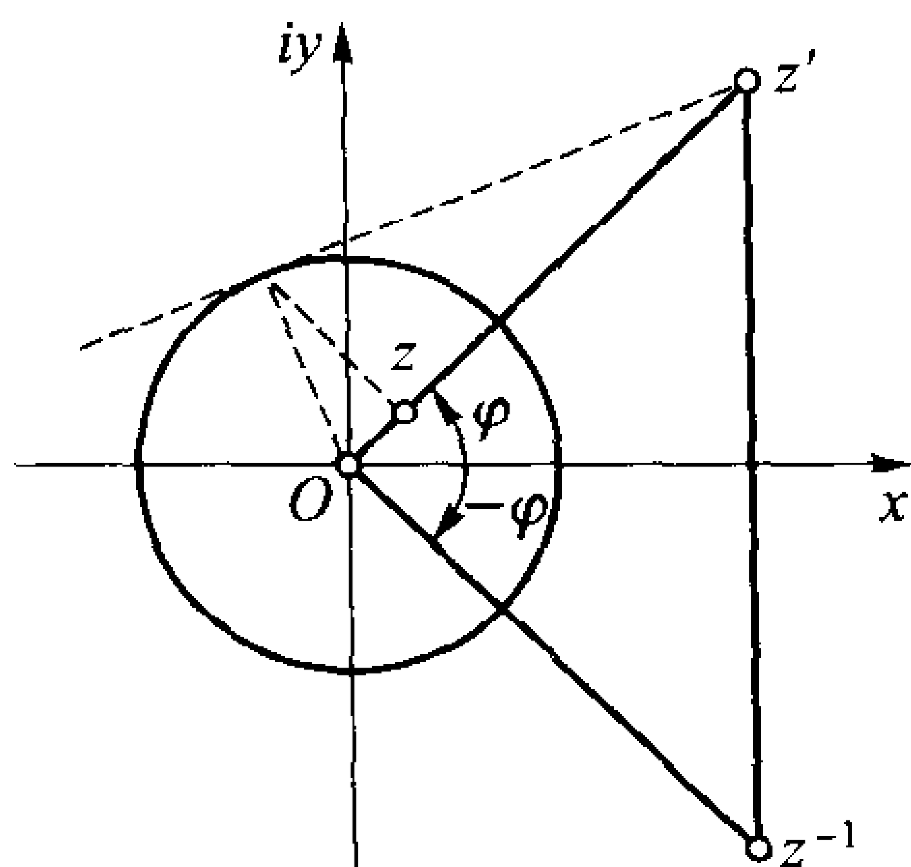


图 20

事实上, 关于积与和模的结论容易直接从定理 1 而不必通过几何直观推导出来. 首先

$$|zz'|^2 = zz'\overline{zz'} = zz'\bar{z}\,\overline{z'} = z\bar{z}\,z'\overline{z'} = |z|^2\,|z'|^2,$$

故 $|zz'| = |z|\cdot|z'|$. 其次, 注意到 $|z| = \sqrt{x^2+y^2} \geqslant \sqrt{x^2} = |x|$, 我们有

$$\begin{aligned} |1+z|^2 &= (1+z)(1+\bar{z}) = 1 + (z+\bar{z}) + z\bar{z} \\ &= 1 + 2x + |z|^2 \leqslant 1 + 2|z| + |z|^2 = (1+|z|)^2, \end{aligned}$$

从而 $|1+z| \leqslant 1 + |z|$. 现在若 $z \neq 0$ 且 $z' \neq 0$, 则

$$\begin{aligned} |z+z'| &= \left|z(1+z^{-1}z')\right| = |z|\cdot\left|1+z^{-1}z'\right| \\ &\leqslant |z|\left(1+\left|z^{-1}z'\right|\right) = |z|\left(1+|z|^{-1}|z'|\right) = |z|+|z'|. \end{aligned}$$

从所得结果可以了解到一个一般的规律: 表示复数的公式 (7) 用于加法的性质比较方便, 而三角形式 (10) 便于得到乘法的性质. 违背了这一规律就会导致特别复杂的计算, 使事情变得模糊起来.

4. 乘方和开方　将复数乘法公式 (12) 写成三角形式可推出 **棣莫弗公式**

$$[r(\cos\varphi + i\sin\varphi)]^n = r^n(\cos n\varphi + i\sin n\varphi) \tag{13}$$

对任意 $n \in \mathbb{Z}$ 成立 (另一种写法是 $|z^n| = |z|^n, \arg z^n = n\cdot\arg z$). 运用公式 (13) 当 $r=1$ 时的特殊情况, 第 1 章 §7 的二项式 (1) 以及关系式

$$i^2 = -1,\ i^3 = -i,\ i^4 = 1,\ i^{4k+l} = i^l$$

可以得到倍角的正弦和余弦

$$\begin{aligned}\cos n\varphi &= \sum_{k\geqslant 0}(-1)^k\begin{pmatrix} n \\ 2k \end{pmatrix}\cos^{n-2k}\varphi\cdot\sin^{2k}\varphi,\\ \sin n\varphi &= \sum_{k\geqslant 0}(-1)^k\begin{pmatrix} n \\ 2k+1 \end{pmatrix}\cos^{n-1-2k}\varphi\cdot\sin^{2k+1}\varphi.\end{aligned} \tag{14}$$

公式 (14) 当 $n=2$ 时的特殊情况我们早已在证明定理 2 的过程中使用过了.

注记 设 $e^{\alpha}=\lim\limits_{n\to\infty}(1+\alpha/n)^n$. 在数学分析中用复函数的幂级数展开证明过 **欧拉公式**

$$e^{i\varphi}=\cos\varphi+i\sin\varphi, \tag{15}$$

注意到

$$e^{i\varphi}e^{i\varphi'}=e^{i(\varphi+\varphi')},\quad \left(e^{i\varphi}\right)^n=e^{in\varphi}.$$

利用欧拉公式可以得到上述所有的结果. 复数 z 的三角形式也可以写成

$$z=|z|\,e^{i\varphi}.$$

下面我们来讨论怎样求一个复数的任意次方根，一个基本的问题是，这样的方根是否永远存在？答案是肯定的，**棣莫弗公式** 对这一问题从本质上给出了完全的解答. 设给定复数 $z=r(\cos\varphi+i\sin\varphi)$, 我们希望找到一个复数 $z'=r'(\cos\varphi'+i\sin\varphi')$, 使得 $(z')^n=z$. 对 $(z')^n$ 使用棣莫弗公式，并比较等式 $(z')^n=z$ 两端的模和辐角，我们有 $(r')^n=r$ 和 $n\varphi'=\varphi+2\pi k$(我们在这里加上一项 $2\pi k$, 是因为辐角只精确到相差 2π 的整倍数). 于是

$$r'=\sqrt[n]{r},\quad \varphi'=\frac{\varphi+2\pi k}{n}$$

($\sqrt[n]{r}$ 指正实数的 n 次算术根). 于是，根 $\sqrt[n]{z}$ 是存在的，但并不唯一确定. 当 $k=0,1,\cdots,n-1$ 时，z' 取 n 个不同的值，它们穷尽了所有可能的根，记 $k=nq+r$, $0\leqslant r\leqslant n-1$, 则有

$$\varphi'=\frac{\varphi+2\pi r}{n}+2\pi q.$$

我们证明了

定理 3 任意复数 $z=|z|(\cos\varphi+i\sin\varphi)$ 开 n 次方总是可能的. z 的全部 n 个 n 次方根分布在以原点为圆心，$\sqrt[n]{|z|}$ 为半径的圆的内接正 n 边形的顶点上：

$$\sqrt[n]{z}=\sqrt[n]{|z|}\left(\cos\frac{\varphi+2\pi k}{n}+i\sin\frac{\varphi+2\pi k}{n}\right), \tag{16}$$

$k=0,1,\cdots,n-1$, □

推论 1 的 n 次方根 (单位根) 由公式

$$\sqrt[n]{1}=\varepsilon_k=\cos\frac{2\pi k}{n}+i\sin\frac{2\pi k}{n} \tag{17}$$

给出， $k=0,1\cdots,n-1$. 它们分布在以原点为圆心， 1 为半径的圆的内接正 n 边形的顶点上. □

从公式 (16) 和 (17) 立即可见，形如 $\sqrt[n]{z}$ 的实根为零个， 1 个或 2 个，而形如 $\sqrt[n]{1}$ 的实根有 1 个或 2 个 (图 21 给出了 1 的 5 次方根).

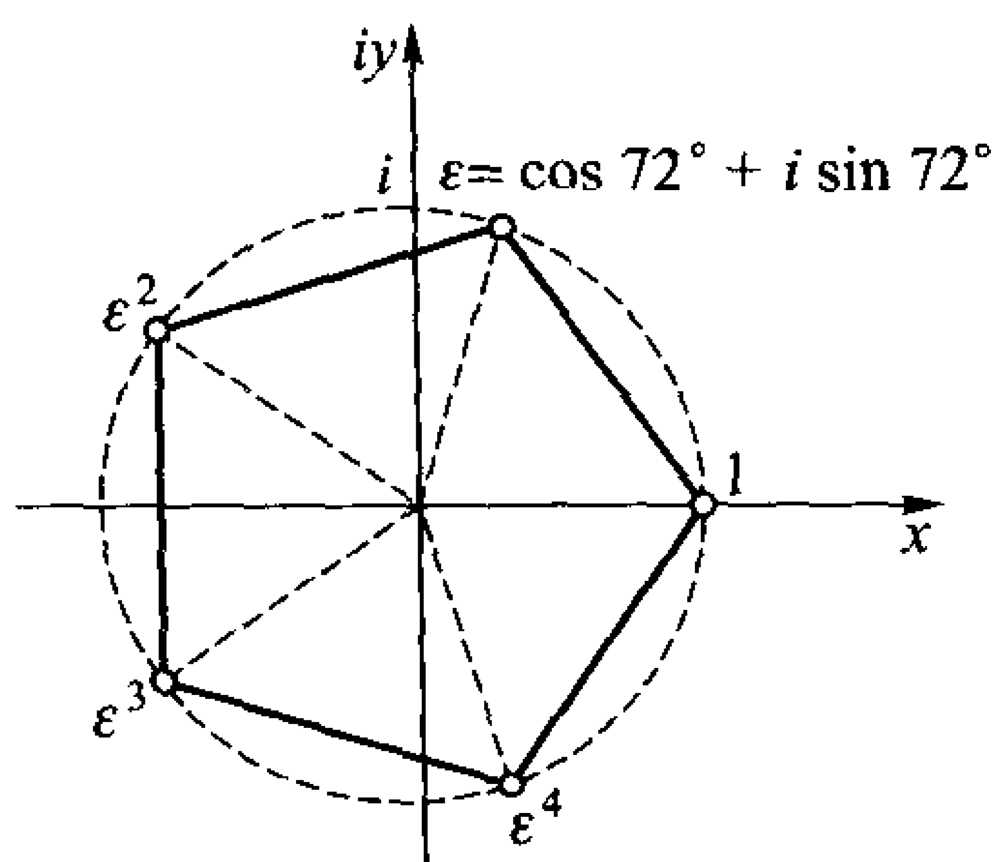


图 21

1 的一个 n 次方根称为**本原的**(或**原的**), 如果它不是 1 的更低次数的方根. 例如

$$\varepsilon=\varepsilon_1=\cos\frac{2\pi}{n}+i\sin\frac{2\pi}{n},\quad \varepsilon_{n-1}$$

是 1 的 n 次本原根.

任意其他的根 ε_k 是本原根的方幂

$$\varepsilon_k=\varepsilon_1^k,$$

这仍然可以从棣莫弗公式看出来. 进一步 $\varepsilon_k\varepsilon_l=\varepsilon_{k+l}$, 其中 $k+l$ 是取模 n 得到的最小非负整数. 特别地， $\varepsilon_k^{-1}=\varepsilon_{n-k}$, $\varepsilon_0=1$. 在学习过群论之后，我们注意到， 1 的 n 次方根构成了一个 n 阶循环群 $\langle\varepsilon\rangle$.

这样就得到了 n 阶循环群的又一个模型. 对于每一个因子 $d|n, \langle\varepsilon\rangle$ 中恰有一个 d 阶子群 $\langle\varepsilon^{n/d}\rangle$. 根 ε_m 是本原的，当且仅当 $\langle\varepsilon_m\rangle=\langle\varepsilon\rangle$, 当且仅当 $\mathrm{Card}\langle\varepsilon^m\rangle=n$, 当且仅当 m 与 n 互素. 例如当 $n=12$ 时， 12 次本原根有 $\varepsilon,\varepsilon^5,\varepsilon^7,\varepsilon^{11}$. 在 $n=p$ 是素数的情况下，所有的异于 1 的根都是本原的. 从代数的观点来看，不计几何位置，所有的 n 次本原根都是等价的.

回到对任意复数 $z\neq 0$ 开 n 次方的问题上来，我们指出， 如果 z' 是某个取定的根(例如 $z'=\sqrt[n]{|z|}(\cos\frac{\varphi}{n}+i\sin\frac{\varphi}{n})$), 则所有其他的根形如 $z'\varepsilon_k$, $k=0,1,\cdots,n-1$. 这一结论与公式 (16) 是一致的.

5. 唯一性定理 复数域 $\mathbb{C}$ 比之于实数域 $\mathbb{R}$ 的优越性我们可以稍后再作充分的评价，但已有的一个事实， $\mathbb{C}$ 包含有 1 的任意次方根就足以提高人们对复数域的兴趣. 我们指出， $\mathbb{C}$ 是 $\mathbb{R}$ 上的 2 维向量空间 (在第 2 章 §1 第 2 段定义的意义下), 基元素可取 $1,i:\mathbb{C}=\langle 1,i\rangle_{\mathbb{R}}$.

一个自然的问题是，具有类似性质的域还有多少？我们有下述唯一性定理.

定理 4 $\mathbb{R}$ 上的任意一个 2 维向量空间 K, 如果还是一个结合，交换，具有单位元 1 且无零因子的环，则必同构于域 $\mathbb{C}$.

证明 不失一般性，将 $1\cdot\mathbb{R}$ 与 $\mathbb{R}$ 等同，并认为 $\mathbb{R}$ 包含在 K 中. 因为 $\dim_{\mathbb{R}} K = 2$, 故存在元素 $e \in K\backslash\mathbb{R}$, 使得 1 和 e 构成向量空间 K 在 $\mathbb{R}$ 上的一个基. 设 $e^2 = \alpha\cdot 1 + 2\beta\cdot e$, 其中 $\alpha, \beta \in \mathbb{R}$, 对于元素 $f = e - \beta \notin \mathbb{R}$, 有 $f^2 = \gamma$, 此处 $\gamma = \alpha + \beta^2 \in \mathbb{R}$. 显然 $\gamma < 0$, 否则 $\sqrt{\gamma} \in \mathbb{R}$, 而 $f = \pm\sqrt{\gamma} \in \mathbb{R}$ 与 $f \notin \mathbb{R}$ 矛盾. 这样存在 $\delta \in \mathbb{R}$, 满足 $\delta^2 = -\gamma^{-1}$. 令 $j = \delta f$, 有 $j^2 = -1$, 且容易验证 (如同对 $\mathbb{C}$ 的作法),K 中的每个非零元可逆，即 K 是域. 映射 $\varphi : \mathbb{C} \to K, x + iy \mapsto x + jy$ 即为所求的域的同构. □

在这一证明中，我们何处用到了 K 是无零因子环这一条件？首先，若没有这个条件，有可能发生 $e^2 = 0$, 从而 $\alpha = \beta = 0, \gamma = 0$ 的情况. 其次，我们断定由 $\gamma \geqslant 0$ 可得 $f = \pm\sqrt{\gamma}$. 而这事实上是因为 $0 = f^2 - \gamma = (f - \sqrt{\gamma})(f + \sqrt{\gamma}) \Rightarrow f - \sqrt{\gamma} = 0$ 或 $f + \sqrt{\gamma} = 0$.

除了 $\mathbb{Q}$ 与 $\mathbb{R}$, 域 $\mathbb{C}$ 还包含有许多其他的子域. 其中特别有趣的是将某个不包含在 $\mathbb{Q}$ 中的 $\mathbb{C}$ 的元素添加到 $\mathbb{Q}$ 上，所得到的域 $\mathbb{Q}$ 的扩张.

例 1(二次域) 设 d 是一个非零整数，可能是负数，使得 $\sqrt{d} \notin \mathbb{Q}$. 域 $\mathbb{Q}(\sqrt{d}) \subset \mathbb{C}$ 当 $d > 0$ 时叫作 **实二次域**, 当 $d < 0$ 时叫作 **虚二次域**. 我们曾在第 4 章 §3 中讨论过域 $\mathbb{Q}(\sqrt{2})$. 在定理 4 中将 j 换成 $\sqrt{d}$, 关系式 $j^2 = -1$ 换成 $(\sqrt{d})^2 = d$, 重复它的证明过程得到

$$\mathbb{Q}(\sqrt{d}) = \left\{a + b\sqrt{d} | a, b \in Q\right\}.$$

特别地，

$$\begin{aligned} (a_1 + b_1\sqrt{d}) + (a_2 + b_2\sqrt{d}) &= (a_1 + a_2) + (b_1 + b_2)\sqrt{d}, \\ (a_1 + b_1\sqrt{d})(a_2 + b_2\sqrt{d}) &= (a_1a_2 + b_1b_2d) + (a_1b_2 + a_2b_1)\sqrt{d}. \end{aligned} \tag{18}$$

其次，若 $a + b\sqrt{d} \neq 0$(即 a, b 不同时为零),

$$(a + b\sqrt{d})^{-1} = \frac{a}{a^2 - db^2} + \frac{b}{a^2 - db^2}\sqrt{d}$$

运用公式 (18) 易验证，映射

$$f : a + b\sqrt{d} \mapsto a - b\sqrt{d}$$

是域 $\mathbb{Q}(\sqrt{d})$ 的自同构，(类似于复共轭映射).

一个数 $\alpha = a + b\sqrt{d}$ 的 **范数** 定义为

$$N(\alpha) = a^2 - db^2 = \alpha f(\alpha).$$

显然，$N(\alpha) = 0 \Leftrightarrow \alpha = 0$. 其次，因为 f 是自同构，

$$N(\alpha\beta) = \alpha\beta f(\alpha\beta) = \alpha\beta f(\alpha)f(\beta) = \alpha f(\alpha)\cdot\beta f(\beta) = N(\alpha)\cdot N(\beta).$$

特别地， $N(\alpha)\cdot N(\alpha^{-1})=N(\alpha\alpha^{-1})=N(1)=1$. 因而范数具备复数域 $\mathbb{C}$ 中模平方的主要性质.

6. 复数的初等几何　实向量空间　$\mathbb{C}=<1,i>_{\mathbb{R}}$ 是欧氏空间：它被赋予了一个正定的数量积

$$(z_1\,|z_2\,)=\mathrm{Re}z_1\bar{z}_2=x_1x_2+y_1y_2,$$

其中 $z_k=x_k+iy_k$, $k=1,2$. 柯西－布尼亚柯夫斯基－施瓦兹不等式成立

$$|(z_1\,|z_2\,)|\leqslant|z_1|\cdot|z_2|,$$

这是因为 $|(z_1\,|z_2\,)|=|\mathrm{Re}z_1\bar{z}_2|\leqslant|z_1\bar{z}_2|=|z_1|\,|\bar{z}_2|=|z_1|\,|z_2|$.

两个向量 (复数) z_1,z_2 叫作 **正交的**, 或 **垂直的**, 若 $(z_1\,|z_2\,)=0$.

从关系式 (12) 不难推出， *两个向量 $z,cz\in\mathbb{C}^*$ 是正交的，当且仅当 c 是纯虚数.*

过点 $u,v\in\mathbb{C}$ 的直线由参数方程

$$w=u+(v-u)t,t\in\mathbb{R},$$

给出. 于是两条直线 $w=u+(v-u)t$ 与 $w'=u'+(v'-u')t$ 的正交性可由关系式 $(v-u\,|v'-u'\,)=0$ 得到. 三个点 $z_1,z_2,z_3\in\mathbb{C},z_1\neq z_2$, 位于同一直线上，当且仅当

$$\frac{z_3-z_2}{z_2-z_1}\in\mathbb{R},\tag{19}$$

即

$$z_3\bar{z}_2-z_3\bar{z}_1-z_1\bar{z}_2\in\mathbb{R}.$$

对直线的正交性作少许讨论. 给出任意一个三角形，为此给定实轴上的两个向量 α,β, 而第三个向量 $i\gamma$ 在虚轴上，易验证三角形的 *三条高交于一点* $i\delta$, 其中 $\delta=-\alpha\beta/\gamma$. 例如验证 $(-\alpha+i\delta\,|-\beta+i\gamma\,)=0$(图 22).

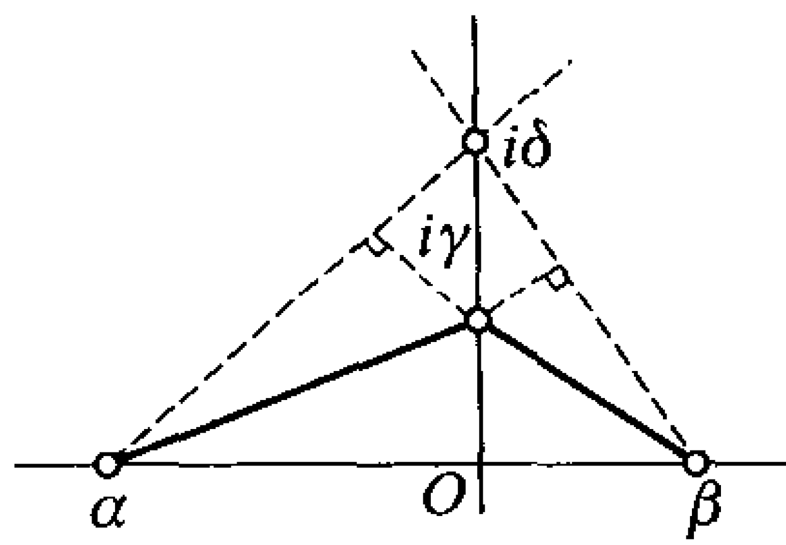


图 22

四个点 z_1,z_2, z_3,$z_4\in\mathbb{C}$, $z_1\neq z_4$, $z_2\neq z_3$ 的 **交比** $[z_1,z_2,z_3,z_4]$ 的概念在许多几何问题中发挥了重要作用. (细节见 [BAII]). 根据定义

$$\begin{aligned}[z_1,z_2,z_3,z_4]&=\frac{z_1-z_2}{z_1-z_4}:\frac{z_3-z_2}{z_3-z_4}\\&=\frac{(z_1-z_2)(z_3-z_4)}{(z_1-z_4)(z_3-z_2)}=\frac{(z_1-z_2)(z_3-z_4)(\bar{z}_1-\bar{z}_4)(\bar{z}_3-\bar{z}_2)}{|z_1-z_4|^2\cdot|z_3-z_2|^2}\end{aligned}\tag{20}$$

是一个复数，依赖于数列 z_1, z_2, z_3, z_4 的排列顺序. 在循环置换下有

$$[z_2, z_3, z_4, z_1] = [z_1, z_2, z_3, z_4]^{-1}.$$

我们指出，关系式 (20) 定义的交比在位移 $T_a: z \mapsto z + a$ 下保持不变. 而三点 z_1, z_2, z_3 不共线这一性质也在位移下不变. 因而 (当计算 $[z_1, z_2, z_3, z_4]$ 时), 以 z_1, z_2, z_3 为顶点的三角形的外接圆的圆心可以放在坐标原点上. 但当 $|z_1| = |z_2| = |z_3|$ 时，易验

$$(z_1 - z_2)(z_3 - z_4)(\bar{z}_1 - \bar{z}_4)(\bar{z}_3 - \bar{z}_2) - i(|z_3|^2 - |z_4|^2) \cdot \mathrm{Im}(z_3\bar{z}_2 - z_3\bar{z}_1 - z_1\bar{z}_2) \in \mathbb{R}$$

(建议读者在本节后面的习题中完成这一验证). 根据 (19) 式，$\mathrm{Im}(z_3\bar{z}_2 - z_3\bar{z}_1 - z_1\bar{z}_2) \neq 0$, 而在这种情况下，乘积 $(z_1 - z_2)(z_3 - z_4)(\bar{z}_1 - \bar{z}_4)(\bar{z}_3 - \bar{z}_2)$ 是实数，或等价地说 (见 (20)), $[z_1, z_2, z_3, z_4]$ 是实数，当且仅当 $|z_3|^2 - |z_4|^2 = 0$, 即 $|z_3| = |z_4|$. 这就意味着 $z_k, 1 \leqslant k \leqslant 4$, 是模相等的四个复数，位于同一个圆周上.

该论断当四个点中的某三点不共线时成立. 我们指出，交比 $[z_1, z_2, z_3, z_4]$ 是实数的性质在序列 z_1, z_2, z_3, z_4 的循环置换下保持不变. 我们证明了下述论断.

定理 5 *设不在同一直线上的四个点 $z_1, z_2, z_3, z_4 \in \mathbb{C}$, $z_1 \neq z_4, z_2 \neq z_3$, 这四点共圆，当且仅当它们的交比是实数.*

这仅仅是用交比的语言得到的诸多几何性质中的一例.

作为本段的结束，我们用几何手段来构造在数学史上占据显著地位的一些新的数域.

例(*可构作性数域*) 在笛卡儿平面上给定两点 (0,0) 和 (1,0). 后面所有的结构仅在圆规和直尺的帮助下实现. 如果构作了点 P 和 Q, 我们自然可以认为连接它们的线段 PQ 也构作出来了. 如果构作了点 P 和线段 r, 那么以 P 为圆心，r 为半径的圆周也可以作出来. 已构作出的两条直线 (线段) 的交点或两个圆的交点的构作也是在这种意义之下.

复数 $a + bi$ 称为 **可构作的**, 如果从点 (0,0) 和 (1,0) 出发，经过有限次上述的 (允许) 构作，我们可以作出点 $P = (a, b)$. 不难看到，$a + bi$ 的可构作性，等价于 $|a|$ 和 $|b|$ 的可构作性. 平面上可在圆规直尺的帮助下构作出来的点的集合，也就是说所有的可构作复数的集合记作 CS.

定理 6 *集合 CS 是域 $\mathbb{C}$ 的子域.*

证明 从数的可构作性定义直接得到，CS 关于加法运算是封闭的 (点 $z + z'$ 是圆心在点 z', 半径为 $|z|$ 与圆心在点 z, 半径为 $|z'|$ 的两个圆的交), 而如果 $z = x + iy \in CS$ 可得 $-z = -x - iy \in CS$.

将长度可构作的线段 $1, \alpha, \beta$ 置于坐标轴上，我们来考察图 23,(a) 和 (b) 中的相似三角形 (虚线代表新的可构作线段), 就得到了积 $\gamma = \alpha\beta$ 和商 $\delta = \alpha/\beta$ 的可构作性. 因为

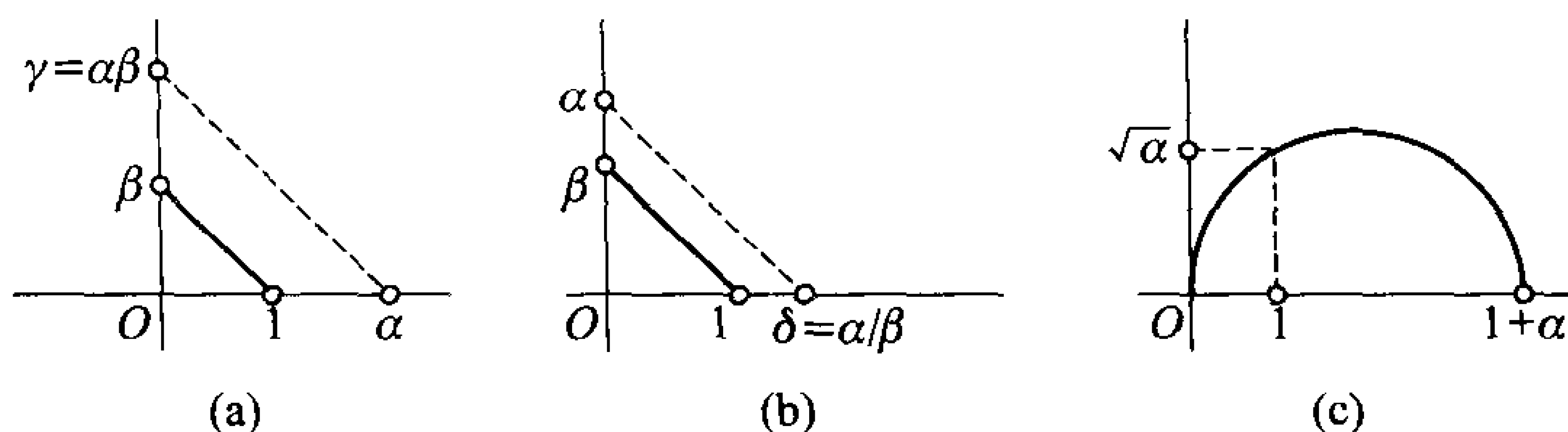


图 23

$$zz' = (x+iy)(x'+iy') = (xx'-yy') + i(xy'+x'y),$$
$$\frac{1}{z} = \frac{x}{x^2+y^2} - i\frac{y}{x^2+y^2}$$

积 zz' 和商 $\frac{1}{z}$ 的可构作性归结为 γ 和 δ 型线段的可构作性. 因而我们证明了集合 CS 关于复数域 $\mathbb{C}$ 的所有的运算都是封闭的. □

注记 1) CS 在复共轭映射 $z \mapsto \bar{z}$ 下不变.

2) 图 23(c) 表明, 可构作实数 $\alpha > 0$ 的二次方根 $\sqrt{\alpha}$ 是可构作的. 这件事对于任意可构作复数 z 亦成立.

CS 的任意子域 $F \subset CS$ 通常称为 **可构作数域**.(显然, $\mathbb{Q} \subset CS$, 且任意可构作数域是特征为零的域. 根据注记 2), 所有的二次域 (见 §5 的例) 是可构作的.

习　　题

1. 找出使 $z^2+(1+i)z$ 为纯虚数的所有模为 1 的复数 z. 在复平面 $\mathbb{C}$ 上画出这些点的轨迹.

2. 设复数 δ 满足方程 $\delta^4=-1$, 域 $\mathbb{R}(\delta)$ 由 $\mathbb{R}$ 添加 δ 得到. 关于 $\mathbb{R}(\delta)$ 我们能说些什么?

3. 设 $A, B \in M_n(\mathbb{R})$. 根据定理 1 证明 $\overline{\det(A+iB)} = \det(A-iB)$(加横线表示复共轭).

4. 设 $A, B \in M_n(\mathbb{R})$,

$$C = \begin{pmatrix} A & B \\ -B & A \end{pmatrix} \in M_{2n}(\mathbb{R}).$$

对实矩阵 C 施行复数域 $\mathbb{C}$ 上的 I 型和 II 型初等变换证明

$$\det C = |\det(A+iB)|^2 .$$

5. (波利亚和塞格). 利用习题 3 和 4 给出下述"奇怪"现象的解释. 带有复系数 $d_{kl} = a_{kl}+ib_{kl}$ 和未知数 $z_i = x_i + iy_i$ 的方形齐次线性方程组

$$\begin{aligned} d_{11}z_1 + \cdots + d_{1n}z_n &= 0, \\ \cdots\cdots\cdots\cdots \\ d_{n1}z_1 + \cdots + d_{nn}z_n &= 0 \end{aligned} \qquad (*)$$

有非平凡解 $(z_1, \cdots, z_n)$, 当且仅当 $\det(d_{kl}) = a+ib = 0$(关于这一点见第 4 章 §3 第 6 段的说明). 这个条件引出了两个方程 $a=0$, $b=0$, 它们联系到 $2n^2$ 个实数值 a_{kl}, b_{kl}. 另一方面, 方程组 $(*)$ 可以写成带有 $2n$ 个实未知数 x_i, y_i 的 $2n$ 个齐次线性方程组. 现在非平凡解存在的条件

是，单独一个 $2n$ 阶实行列式等于零，它仅由关于 a_{kl}, b_{kl} 的一个方程给出. 这两个结果是怎样相容的？

6. 找出二次域 $\mathbb{Q}(\sqrt{d})$ 的自同构，它应该保持有理数不变.

提示： 恒等映射和映射 $a+b\sqrt{d}\mapsto a-b\sqrt{d}$.

7. 当 $n>1$ 时，1 的所有 n 次方根的和等于什么？求 1 的 12 次本原根的和，以及 15 次本原根的和.

8. 证明 $\zeta=(2+i)/(2-i)$ 不是 1 的根，尽管 $|\zeta|=1$.

提示： $\zeta^n=1\Rightarrow(2-i)^n=(2+i)^n=(2-i+2i)^n=(2-i)^n+\cdots+(2i)^n\Rightarrow(2-i)(a+bi)=(2i)^n\Rightarrow 5(a^2+b^2)=2^{2n}\Rightarrow 5|2^{2n}$, 得到矛盾.

9. 集合 $S^1=\{e^{i\varphi}|\varphi\in\mathbb{R}\}$(以 1 为半径的圆周) 组成 $\mathbb{C}$ 的乘法群 $(\mathbb{C}^*,\cdot)$ 的一个子群. 任意 $\mathbb{R}-$ 线性映射 $f:\mathbb{C}\to\mathbb{C}$ 叫作 **正交的**, 若 $(f(z)|f(z'))=(z|z')$, 即若 f 保存向量的长度 (两点间的距离). 证明如果 $f(z)=cz$ 或 $f(z)=c\bar{z}$, 其中 $c\in S^1$, 则 $f:\mathbb{C}\to\mathbb{C}$ 是正交的.

10. 证明

$$\begin{vmatrix} x_0 & x_1 & x_2 & \cdots & x_{n-1} \\ x_{n-1} & x_0 & x_1 & \cdots & x_{n-2} \\ x_{n-2} & x_{n-1} & x_0 & \cdots & x_{n-3} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ x_1 & x_2 & x_3 & \cdots & x_0 \end{vmatrix} = \prod_{k=0}^{n-1}(x_0+\zeta^k x_1+\zeta^{2k}x_2+\cdots+\zeta^{(n-1)k}x_{n-1}),$$

其中 ζ 是 1 的一个 n 次本原根.

§2 多项式环

我们在第 2 章和第 3 章讨论过线性方程组的理论，与之类似，多项式理论也是传统代数学的一个古老而出色的研究领域. 多种数学问题都可以用多项式的语言陈述和解决. 原因是多方面的，其中之一在于多项式环的 “泛性”, 我们将在第 1 段中对它进行讨论.

设 R 是有单位元 1 的交换环 (像往常一样是结合的),A 是 R 的某个子环，且包含 1. 如果 $t\in R$, 则 R 中包含有 A 和 t 的最小子环显然由形如

$$a(t)=a_0+a_1t+a_2t^2+\cdots+a_nt^n \qquad (*)$$

的元素组成，其中 $a_s\in A$, $n\in\mathbb{Z}$, $n\geqslant 0$. 我们将它记作 $A[t]$, 并称之为从 A 添加元素 t 得到的环，表达式 (*) 叫作系数在 A 中的 t 的多项式. 看几个例子 (如 $n=2$) 就可以知道如何计算多项式的和与积：

$$\begin{aligned} a(t)+b(t) &= (a_0+a_1t+a_2t^2)+(b_0+b_1t+b_2t^2) \\ &= (a_0+b_0)+(a_1+b_1)t+(a_2+b_2)t^2, \\ a(t)\cdot b(t) &= a_0b_0+(a_0b_1+a_1b_0)t+(a_0b_2+a_1b_1+a_2b_0)t^2 \\ &\quad +(a_1b_2+a_2b_1)t^3+a_2b_2t^4. \end{aligned}$$

显然，合并同类项基于所有的元素 a_i, b_j, t^k 是两两可交换的.

回忆 t 是随机地从 R 中取出的一个元素，因而外表不同的表达式 (*) 可能实质上是完全一样的. 如果令 $A=\mathbb{Q}$, $t=\sqrt{2}$, 则 $t^2=2$, 而 $t^3=2t$, 但这两个关系式不可能从多项式的任何形式规则中推导出来. 为了得到我们熟悉的多项式的概念，必须去除所有附带的关系，将 t 当作一个任意的符号，它不一定包含在 R 中. 符号叫作什么是不重要的. 重要的是表达式 $a(t)+b(t)$, $a(t)b(t)$ 中系数的构成法则. 现在我们来给出作为代数对象的多项式和这些对象构成的多项式环的精确定义.

1. 单变元多项式 设 A 是任意有单位元的交换环. 构造一个新的环 B, 它的元素是无穷序列

$$f=(f_0, f_1, f_2, \cdots),\ f_i \in A, \tag{1}$$

除有限多项之外，所有的 f_i 都等于零. 我们来定义 B 上的加法和乘法运算，令

$$\begin{aligned} f+g &= (f_0, f_1, f_2, \cdots)+(g_0, g_1, g_2, \cdots) \\ &= (f_0+g_0, f_1+g_1, f_2+g_2, \cdots), \\ f\cdot g &= h=(h_1, h_2, h_3, \cdots), \end{aligned}$$

其中 $h_k=\sum\limits_{i+j=k} f_i g_j$, $k=0,1,2,\cdots$.

显然，作加法和乘法的结果仍然是形如 (1) 的序列，仅含有限多个非零项，即所得的元素包含在 B 中. 验证环的公理 (见第 4 章 §3), 除结合律外，其余各条都是显然的. 事实上，因为 B 中两个元素相加归结为环 A 中的有限个元素相加，$(B,+)$ 是一个交换群，有零元素 $(0,0,0,\cdots)$ 且任意元素 $f=(f_0, f_1, f_2, \cdots)$ 有负元素 $-f=(-f_0, -f_1, -f_2, \cdots)$. 其次，乘法是交换的，因为 h_k 通过 f_i 和 g_j 的表达式是对称的. 用这一表达式也可证明 B 满足分配律 $(f+g)h=fh+gh$. 关于乘法运算的结合律，设

$$f=(f_0, f_1, f_2, \cdots),\ g=(g_0, g_1, g_2, \cdots),\ h=(h_0, h_1, h_2, \cdots)$$

是集合 B 中的任意三个元素. 若 $fg=d=(d_0, d_1, d_2, \cdots)$, 其中 $d_l=\sum\limits_{i+j=l} f_i g_j, l=0,1,2,\cdots$, 则 $(fg)h=dh=e=(e_0, e_1, e_2, \cdots)$, 其中 $e_s=\sum\limits_{l+k=s} d_l h_k=\sum\limits_{l+k=s}(\sum\limits_{i+j=l} f_i g_j)h_k$ $=\sum\limits_{i+j+k=s} f_i g_j h_s$. 计算 $f(gh)$ 得到同样的结果. 于是 B 是一个带有单位元 $(1,0,0,\cdots)$ 的交换结合环.

序列 $(a,0,0,\cdots)$ 可以像 A 中的元素一样相加和相乘. 这就使我们可以将这些序列与环 A 中的对应元素等同起来，即对任意的 $a\in A$, 令 $a=(a,0,0,\cdots)$. 于是 A 成为 B 的一个子环.

其次，我们将序列 $(0,1,0,0,\cdots)$ 记作 X, 称之为 A 上的 **变元**(或 **未定元**). 运用 B 中的乘法运算，我们求出

$$\begin{aligned} X &= (0,1,0,0,\cdots) \\ X^2 &= (0,0,1,0,\cdots) \\ &\cdots\cdots\cdots\cdots \\ X^n &= (0,0,\cdots,0,1,0,\cdots) \end{aligned} \tag{2}$$

此外，根据 (2) 式和包含关系 $A \subset B$, 我们有

$$(0,0,\cdots,0,a,0,\cdots) = aX^n = X^n a.$$

于是，如果 f_n 是序列 $f = (f_0, f_1, \cdots, f_n, 0, 0, \cdots)$ 的最后一个非零项，则在新的记号下

$$\begin{aligned} f &= (f_0,\cdots,f_{n-1},0,0,\cdots) + f_n X^n \\ &= (f_0,\cdots,f_{n-2},0,0,\cdots) + f_{n-1}X^{n-1} + f_n X^n \\ &\cdots\cdots\cdots\cdots \\ &= f_0 + f_1 X + f_2 X^2 + \cdots + f_n X^n. \end{aligned} \tag{3}$$

元素 f 的这种表达式是唯一的,因为 (3) 式右边的 $f_0,\cdots,f_n$ 是序列 $(f_0,\cdots,f_n,0,\cdots)$ 的项，$f=0$, 当且仅当 $f_0=\cdots=f_n=0$.

定义 上述环 B 记作 $A[X]$，叫作 A 上 **单变元 X 的多项式环**, 它的元素叫作 **多项式**.

当然，将一个固定的符号 X 称为变元或未定元并非术语上的恰当发明，但这已成为习惯，不会导致误解.

我们有意识地使用大写字母 X 是为了将专有的多项式表达式 $f = X$ 与函数论中的变量 x 特别区分开来，后者遍历某个定义域 (纯粹是临时约定，以后不一定遵守). 更经常地是将多项式 f 写成下述形式

$$f(X) = a_0 X^n + a_1 X^{n-1} + \cdots + a_n,$$

即按照 X 的降幂排列. 今后我们将根据方便与否来决定书写的形式.

元素 f_i (或 a_i) 叫作多项式 f 的 **系数**. 若 f 的全部系数都等于零, 则称 f 为 **零多项式**. X 的零次方幂的系数 f_0 叫作 **常数项**. 如果 $f_n \neq 0$, 则 f_n 称为 **首项** 系数, 而 n 叫作多项式的 **次数**, 记作 $n = \deg f$. 约定零多项式的次数是 $-\infty$,($-\infty+(-\infty)=-\infty$, 对任意 $n\in\mathbb{N}$,$-\infty+n=-\infty$,$-\infty<n$). 次数为 1,2,3 的多项式分别叫作 **线性的, 二次的, 三次的** 多项式.

环 A 的单位元 1 是环 $A[X]$ 的单位元，它是一个零次多项式. 根据 $A[X]$ 中加法和乘法的定义立刻推出，对于次数为 n 和 m 的任意两个多项式

$$f = f_0 + f_1 X + \cdots + f_n X^n, \quad g = g_0 + g_1 X + \cdots + g_m X^m \tag{4}$$

分别有不等式

$$\deg(f+g) \leqslant \max(\deg f, \deg g), \deg(fg) \leqslant \deg f + \deg g \tag{5}$$

只要 (4) 式中的两个多项式的首项系数的乘积 $f_n g_m$ 不等于零，不等式 (5) 中的第二个式子就是一个等式

$$\deg(fg) = \deg f + \deg g$$

因为

$$fg = f_0g_0 + (f_0g_1 + f_1g_0)X + \cdots + (f_ng_m)X^{n+m} \tag{6}$$

这事实意味着下述

定理 1　*如果 A 是整环，则 $A[X]$ 也是整环.* □

多项式环在交换环中的地位在某种程度上可以解释如下：

定理 2　*设交换环 R 包含有 A 作为子环. 对于任意元素 $t \in R$，存在唯一的环同态 Π_t: $A[X] \to R$，使得*

$$\forall\, a \in A, \quad \Pi_t(a) = a, \quad \Pi_t(X) = t \tag{7}$$

证明　首先假设这样的同态 Π_t 存在. 给定写成 (3) 式的任意多项式 f，因为对于 f 的每个系数 $f_i, \Pi_t(f_i) = f_i$，且 $\Pi_t(X^k) = (\Pi_t(X))^k = t^k$ (同态的性质和条件 (7))，所以

$$\begin{aligned}\Pi_t(f) &= \Pi_t(f_0 + f_1X + \cdots + f_nX^n) \\ &= f_0 + f_1t + \cdots + f_nt^n,\end{aligned} \tag{8}$$

即 $\Pi_t(f)$ 是唯一确定的，并由公式 (8) 给出. 反之，如果我们用公式 (8) 定义一个映射 Π_t，则 Π_t 显然满足条件 (7) 并得到一个环同态. 事实上，Π_t 作为环的加法群的同态是清楚的，至于乘法，将 Π_t 应用到乘积 (6)，则 (广义) 分配律给出

$$\begin{aligned}\Pi_t(fg) &= f_0g_0 + (f_0g_1 + f_1g_0)t + \cdots + (f_ng_m)t^{n+m} \\ &= \left(\sum_{i=1}^{n} f_it^i\right)\left(\sum_{j=1}^{m} g_jt^j\right) = \Pi_t(f)\cdot\Pi_t(g).\end{aligned}$$ □

将公式 (8) 定义的映射 Π_t 作用到多项式 $f = f(X)$ 上，其结果称为在 f 中用 t **替换** X，或简单地 (带有某种牵强) 称为 f 在 $X = t$ 时的值，因而记作 $\Pi_t(f) = f(t)$. 知道了 $\Pi_t(f)$，就意味着能够计算 f 在 $X = t$ 时的值. 令 $x \in A$，同态 Π_x 乃是联系多项式研究中的函数观点与代数观点的一个纽带. 根据定义，线性多项式 $X - c = (-c, 1, 0, \ldots)$ 不等于零，但与之相关联的多项式函数 $x \mapsto x - c$ 当 $x = c$ 时取零值. 另一个例子：系数取自域 $\mathbb{F}_2$ (其中 $1 + 1 = 0$) 的非零多项式 $X^2 + X$ 给出了一个零函数 $\tilde{f}$：$\mathbb{F}_2 \to \mathbb{F}_2$，因为 $0^2 + 0 = 0$ 和 $1^2 + 1 = 0$.

元素 $t\in R$ 称为 A 上的 **代数元**, 若存在 $f\in A[X]$, 使得 $\Pi_t(f)=0$. 如果 $\Pi_t{:}A[X]\to R$ 是一个同构嵌入 (单同态), 则 t 叫作 A 上的 **超越元**. 当 $A=\mathbb{Q},R=\mathbb{C}$ 时, 则简单地称之为 **代数数** 和 **超越数**. 例如在数学分析中定义的数 e 和 π 是超越的, 而数 $\sqrt{2},\sqrt{3}$, $\sqrt{2}+\sqrt{3}$ 是代数的.

同态 Π_t 原本用于反映多项式环 $A[X]$ 的 *泛性*. 现在多项式环泛性的更完备的刻画如下.

定理 3 *设 A 和 R 是任意交换环, t 是 R 的一个元素, 而 $\varphi{:}A\to R$ 是环同态. 则 φ 可以唯一地扩充为环同态 φ_t: $A[X]\to R$, 它将变元 X 对应到 t.*

定理 3 的证明在本质上与定理 2 的证明类似, 留给读者作为习题.

2. 多变元多项式 当 $A\subset R$ 时, 如果在本节开头的考察中取任意 n 个元素 $t_1,\cdots,t_n\in R$, 并考虑 R 中包含有 A 和 $t_1,\cdots,t_n$ 的所有子环的交, 则我们得到一个环 $A[t_1,\cdots,t_n]$. 如同 $n=1$ 的情况, 其元素的形式记法暗示着引入 n 变元多项式的必要性. 作法非常简单. 回忆构造环 $B=A[X]$ 是从带有单位元 1 的交换环 A 开始的. 现在我们可以用环 B 代替 A, 构造环 $C=B[Y]$, 其中 Y 是一个新的变元, Y 对 B 所起的作用, 与 X 对 A 一样. C 的元素可唯一地写成 $\sum b_jY^j$, $b_j\in B$ 的形状, 且 B 等同于 C 的一个子环, 由形如 $bY^0=b\cdot 1$ 的元素组成. 因为元素 $b_j\in B$ 可唯一地表示成 $b_j=\sum a_{ij}X^i$, 故 C 中的任意元素形如

$$\sum_{i=0}^{k}\sum_{j=0}^{l}a_{ij}X^iY^j,\quad a_{ij}\in A,$$

并且根据构造法, a_{ij} 与 X 和 Y 可交换, 变元 X 与 Y 可交换. C 叫作 A 上两个变元 (或未定元)X,Y 的 **多项式环**.

将这种构造重复充分多次, 我们就得到了 A 上 n 变元 (或未定元) $X_1,\cdots,X_n$ 的多项式环 $A[X_1,\cdots,X_n]$.

我们约定, 将 n 个非负整数 $i_1,\cdots,i_n$ 的序列 $(i_1,\cdots,i_n)\in\overline{\mathbb{N}}^n(\overline{\mathbb{N}}=\mathbb{N}\cup\{0\})$ 简记作 (i). 这时任意元素 $f\in A[X_1,\cdots,X_n]$ 可写成如下形式:

$$f=\sum_{(i)}a_{(i)}X^{(i)},\quad a_{(i)}\in A,\tag{9}$$

其中 $X^{(i)}=X_1^{i_1}\cdots X_n^{i_n}$ 是一个单项式, f 是系数取自 A 的单项式的线性组合. 根据多项式的定义, (9) 式中所有的系数 $a_{(i)}$ 除有限多个以外都等于零. 写法 (9) 的唯一性可直接从下述论断得到.

多项式 f 等于零, 当且仅当所有的系数 $a_{i_1\cdots i_n}$ 等于零. 当 $n=1$ 时, 在构造环 $A[X]$ 的过程中已发现了这一结果. 当 $n>1$ 时, 对 n 作最简单的归纳. 即我们可以将多项式写成

$$f=\sum a_{i_1\cdots i_n}X_1^{i_1}\cdots X_n^{i_n}=\sum_{i_n}b_{i_n}X^{i_n},$$

其中

$$b_{i_n} = \sum_{i_1,\cdots,i_{n-1}} a_{i_1\cdots i_{n-1}i_n} X_1^{i_1}\cdots X_{n-1}^{i_{n-1}}$$

是变元较少的多项式. 对 $n=1$ 的结论和归纳假设表明,

$$f=0, \quad \Leftrightarrow \forall i_n, b_{i_n}=0 \Leftrightarrow \forall (i_1,\cdots,i_n) \quad a_{i_1\cdots i_{n-1}i_n}=0.$$

现在自然可以认为, 两个多项式 $f,g\in A[X_1,\cdots,X_n]$ 相等, 当且仅当它们的相同单项式的系数相等 (根据上面所述,

$$(i_1,\cdots,i_n)\neq(j_1,\cdots,j_n) \Rightarrow X_1^{i_1}\cdots X_n^{i_n}\neq X_1^{j_1}\cdots X_n^{j_n}).$$

多项式 f 关于 X_k 的 **次数** 记作 $\deg_k f$, 它是在所有 $a_{(i)}\neq 0$ 的单项式 $a_{(i)}X^{(i)}$ 中, X_k 的指数中的最大整数. 例如多项式 $1+X+XY^3+X^2Y^2$ 关于 X 的次数是 2, 关于 Y 的次数是 3.

整数 $i_1+\cdots+i_n$ 叫作 **单项式** $X_1^{i_1}\cdots X_n^{i_n}$ 的 **(全) 次数**.

多项式 f 的次数(或 **全次数**)$\deg f$ 是它的单项式全次数中的最大值. 令 $\deg 0=-\infty$. 在多变元的情况下, 谈论多项式的首项是没有意义的, 因为全次数最大的单项式可能有许多个.

我们在第 1 段中对 $A[X]$ 得到的许多结果可以转移到环 $A[X_1,\cdots,X_n]$ 上. 例如运用定理 1 并对 n 作归纳立即得到

定理 1′　*如果 A 是整环, 则环 $A[X_1,\cdots,X_n]$ 也是整环. 特别地, 任意域 P 上的 n 变元多项式环是整环.*

下述论断可看作定理 1′ 的一个有效的改进.

定理 4　*设 f 和 g 是整环 A 上的任意两个 n 变元多项式. 则*

$$\deg(fg)=\deg f+\deg g.$$

证明　一个多项式 $h(X_1,\cdots,X_n)$ 叫作 m 次 **齐次多项式** 或 **m次形式**, 如果它所有的单项都有同一个全次数 m,1,2,3 次形式分别称为 **线性**, **二次** 和 **三次形式**. 如果将 f 中所有次数相同的单项式 (仅考虑有非零系数的单项式) 合并在一起, 我们就把多项式 $f=\sum a_{(i)}X^{(i)}$ 唯一地表示成次数各不相同的形式 f_m 的和

$$f=f_0+f_1+\cdots+f_k, k=\deg f.$$

如果

$$g=g_0+g_1+\cdots+g_l, l=\deg g,$$

则显然,

$$fg=f_0g_0+(f_0g_1+f_1g_0)+\cdots+f_kg_l$$

(这个式子与 (6) 式类似, 但 f_i, g_j 有另外的含义), 从而 $\deg fg \leqslant k+l$. 根据定理 1′, 从 $f_k \neq 0, g_l \neq 0$ 得到 $f_k g_l \neq 0$, 即 $\deg(fg) = \deg(f_k g_l) = k+l = \deg f + \deg g$.□

3. 带余除法 在第 1 章 §9 第 3 段中对整数 $\mathbb{Z}$ 引入过带余除法. 当 A 是整环时, 完全类似的算法可以在环 $A[X]$ 中进行 (当 $A = \mathbb{R}$ 时, 初等代数中已有这一算法: 回忆带余除法).

定理 5 *设 A 是整环, g 是 $A[X]$ 中的多项式, 其首项系数在 A 中可逆. 那么对于每一个多项式 $f \in A[X]$, 存在唯一的一对多项式 $q, r \in A[X]$, 使得*

$$f = qg + r, \deg r < \deg g. \tag{10}$$

证明 设

$$f = a_0X^n + a_1X^{n-1} + \cdots + a_n,$$
$$g = b_0X^m + b_1X^{m-1} + \cdots + b_m,$$

其中 $a_0b_0 \neq 0$, 且 $b_0 | 1$. 对 n 作归纳. 若 $n = 0$, 且 $m = \deg g > \deg f = 0$, 则令 $q = 0, r = f$. 若 $n = m = 0$ 则令 $r = 0$ 和 $q = a_0b_0^{-1}$. 我们假设定理对所有次数 $< n$ 的多项式成立, 此处 $n > 0$. 不失一般性, 设 $m \leqslant n$, 因为在相反的情况下, 取 $q = 0$ 且 $r = f$ 即可. 这时

$$f = a_0b_0^{-1}X^{n-m} \cdot g + \bar{f},$$

其中 $\deg \bar{f} < n$. 根据归纳假设, 我们能够找到 $\bar{q}$ 和 r, 使得 $\bar{f} = \bar{q}g + r$, 并且 $\deg r < m$. 令

$$q = a_0b_0^{-1}X^{n-m} + \bar{q},$$

我们就得到了具有所需性质的一对多项式 q 和 r.

还需证明商 q 和余 r 的唯一性, 我们设

$$qg + r = f = q'g + r'$$

则 $(q' - q)g = r - r'$. 根据定理 1, 有 $\deg(r - r') = \deg(q' - q) + \deg g$, 在我们的条件下, 仅有的可能性为 $r' = r$ 且 $q' = q$ (回忆 $\deg 0 = -\infty$ 以及 $-\infty + m = -\infty$).

最后指出, 商 q 和余 r 的系数属于完全相同的环 A, 即 $f, g \in A[X] \Rightarrow q, r \in A[X]$. □

注记 首项系数为 1 的多项式通常称为**首一多项式**. 上述用多项式 g 去除 f 的过程叫作**欧几里得算法**, 若 g 为首一多项式, 则算法略为简单. 若 (10) 式中的余 r 等于零 $f = qg$, 则称 f 被 g**整除**.

习 题

1. 多项式 $f(X) = X^5 + 3X^4 + X^3 + 4X^2 - 3X - 1$, $g(X) = X^2 + X + 1$ 可以看作环 $\mathbb{Z}[X]$ 中的多项式或者环 $\mathbb{Z}_5[X]$ 中的多项式. 用带余除法证明, 在第一种情况下 $f(x)$ 不被 $g(x)$ 整除, 而在第二种情况下, $f(x)$ 可以被 $g(x)$ 整除. 与此相反的情况有可能出现吗?

2. 用定理 3 证明，如果 F 是域，则环 $F[X]$ 的保持 F 不变的所有的自同构组成的群同构于变换群 $X \mapsto aX+b$, 其中 $a, b \in F$, $a \neq 0$.

3. 证明多项式 $f \in F[X_1, \cdots, X_n]$ 是 m 次形式 (参看定理 4 的证明)，当且仅当 $f(tX_1, \cdots, tX_n) = t^m f(X_1, \cdots, X_m)$，其中 t 是一个新的变元.

4. 证明全次数为 m 的 n 变元单项式的个数为 $\begin{pmatrix} m+n-1 \\ m \end{pmatrix}$.

提示：利用在 n 和 m 上的双重归纳法，借助关系式

$$\binom{m+(n-1)-1}{m} + \binom{(m-1)+n-1}{m-1} = \binom{m+n-1}{m}.$$

5. 返回第 1 段的定义，考察集合 $A[[X]]$，它由变元 (或未定元)X 的**形式幂级数** $f(X) = \sum_{i \geqslant 0} a_i X^i$ 组成，或者由序列 $(a_0, a_1, a_2, \cdots)$ 组成，其中系数 a_i 是交换环 A 中的任意元素，可能有无限多个 $a_i \neq 0$. $A[[X]]$ 中的形式幂级数的运算与多项式的运算遵循同样的法则：

$$\left(\sum a_i X^i\right) + \left(\sum b_i X^i\right) = \sum (a_i + b_i) X^i,$$
$$\left(\sum a_i X^i\right)\left(\sum b_j X^j\right) = \sum c_k X^k, c_k = \sum_{i+j=k} a_i b_j$$

证明集合 $A[[X]]$ 连同这些运算构成一个交换结合环，带有单位元 $1 = (1, 0, 0, \cdots)$.

因为在幂级数 $f = \sum a_i X^i$ 中，变元 X 有任意大的方幂 X^i, 那么谈论次数 $\deg f$ 就没有意义了，比较自然的是考察 f 的级 $\omega(f)$, 它是使 $a_n \neq 0$ 的最小下标 n(令 $\omega(0) = +\infty$).

证明

i) $\omega(f+g) \geqslant \min\{\omega(f), \omega(g)\}$;

ii) $\omega(fg) \geqslant \omega(f) + \omega(g)$.

如果 A 是一个整环，证明 $\omega(fg) = \omega(f) + \omega(g)$. 特别地这时 $A[[X]]$ 也是整环.

证明 $A[X]$ 是 $A[[X]]$ 的一个子环.

6. 多项式和幂级数经常用来作为各种类型的数值的**生成函数**. 我们用两个简单的例子说明这一点.

a) 用 $\mathbb{Z}[X]$ 中的二项公式 $\sum \binom{n}{i} X^i = (1+X)^n$ 和显然的分解 $(1+X)^m(1+X)^n = (1+X)^{m+n}$ 证明关系式

$$\sum_{i=0}^{k} \begin{pmatrix} m \\ i \end{pmatrix} \begin{pmatrix} n \\ k-i \end{pmatrix} = \begin{pmatrix} m+n \\ k \end{pmatrix}.$$

b) 在带有二元运算的集合中，可以在 n 个元素的乘积之间安插括号，求出所有可能的安插方式的数目 l_n, 为此引入生成函数 —— 形式幂级数

$$l(X) = \sum_{n \geqslant 1} l_n X^n = X + X^2 + 2X^3 + \cdots,$$

是有用的. 它的前几个系数在第 4 章 §1 第 3 段中已经计算过. 从显然的递推关系

$$l_n = \sum_{k=1}^{n-1} l_k l_{n-k}$$

得到 $l(X)^2 = l(X) - X$. 解这个二次方程，我们有

$$l(X) = \frac{1-\sqrt{1-4X}}{2}$$

(根式前的符号是由条件 $l_n > 0$ 决定的). 但是如果幂级数 $f(X)$ 满足 $f^r = 1 + \lambda X, r \in \mathbb{N}$, 则

$$f(X) = 1 + \sum_{k=1}^{\infty}\left[\prod_{i=0}^{k-1}\left(\frac{1}{r} - i\right)\right]\frac{(\lambda X)^k}{k!}$$

(姑且认为泰勒展开式存在). 在我们的情况下 $r = 2$, $\lambda = -4$, 且简单的代换给出了最后的表达式

$$l_n = \frac{1}{n}\binom{2n-2}{n-1}$$

(我们指出 $l_n = C_{n-1}$ 是经典的 **卡塔兰数**).

建议补上所有的中间步骤.

§3 多项式环中的因式分解

1. 整除的初等性质 从第 1 章开始，我们在几个地方涉及整数环 $\mathbb{Z}$ 中的整除性问题，但是暂时还没有证明算术基本定理. 现在到了填补这一空白，并且将结论推广到更广泛的环类上的时候. 我们首先感兴趣的是域 P 上的多项式环 $P[X]$.

我们从任意的整环 R 入手. R 中的可逆元在前文叫作 1 的因子. 有时也称为**正则元**. 显然，多项式 $f \in A[X]$ 是可逆的 (正则的), 当且仅当 $\deg f = 0$, 并且 $f = f_0$ 是 A 中的可逆元，因为 $fg = 1 \Rightarrow \deg f + \deg g = \deg 1 = 0$.

我们称元素 $b \in R$ 被元素 $a \in R$ **整除** (或 b 是 a 的 **倍数**), 如果存在元素 $c \in R$, 使得 $b = ac$ (记作 $a|b$). 如果 $a|b$, $b|a$ 同时成立，则 a 和 b 叫作 **相伴元**. 这时 $b = ua$, 其中 $u|1$. 根据上面的说明，多项式 $f, g \in A[X]$ 是相伴的，当且仅当它们仅相差 A 中的一个可逆因子.

元素 $p \in R$ 叫作 **素元**(或 **既约元**), 如果 p 是不可逆的，且不能表成 $p = ab$ 的形式，其中 a, b 均为非可逆元，因为域 P 中的每一个非零元都是可逆的，故 P 中没有素元. 环 $A[X]$ 中的素元叫作 **既约多项式**.

我们列出在一个整环 R 中整除性的下述基本性质.

1) 如果 $a|b$, $b|c$, 则 $a|c$. 事实上，我们有 $b = ab', c = bc'$, 其中 $b', c' \in R$. 所以 $c = (ab')c' = a(b'c')$.

2) 如果 $c|a$ 且 $c|b$, 则$c|(a \pm b)$. 事实上，根据条件，$a = ca', b = cb'$ 其中 $a', b' \in R$, 由分配律得到 $a \pm b = c(a' \pm b')$.

3) 如果 $a|b$, 则$a|bc$. 显然 $b = ab' \Rightarrow bc = (ab')c = a(b'c)$.

结合 2) 与 3), 我们有

4) 如果元素 $b_1, b_2, \cdots, b_m \in R$ 都能被 $a \in R$ 整除，则 $b_1c_1 + b_2c_2 + \cdots + b_mc_m$ 也能被 a 整除，其中 $c_1, c_2, \cdots, c_m$ 是 R 中的任意元素.

定义 整环 R 叫作**唯一因子分解环**, 若 R 中的任意元素 $a\neq 0$ 可表成下述形式:

$$a = up_1p_2\dots p_r, \tag{1}$$

其中 u 是可逆元, $p_1,p_2,\dots,p_r$ 是素元 (不必两两不等), 并且如果存在另一个分解 $a=vq_1q_2\dots q_s$, 则 $r=s$, 适当地选取 p_i 和 q_j 的下标, 有

$$q_1 = u_1p_1, \ \dots \ , \ q_r = u_rp_r,$$

其中 $u_1,\dots,u_r$ 是可逆元.

假设在等式 (1) 中允许 $r=0$, 我们约定, R 中的可逆元素也有素因子分解, 尽管它是平凡的. 显然, 如果 p 是素元, u 是可逆元, 则与 p 相伴的元素 up 也是素元. 在环 $\mathbb{Z}$ 中有可逆元 1 和 -1, $\mathbb{Z}$ 中的序 $(a<b)$ 使我们可以从两个相伴的素元 $\pm p$ 中选择正素元 p. 在环 $P[X]$ 中, 考察首一既约多项式 (见 §2 最后的注记) 比较方便.

下述的一般论断成立.

定理 1 设 R 是一个整环, 其中的每一个元素都有素因子分解. 则 R 中的分解是唯一的 (即 R 是唯一因子分解环), 当且仅当每一个整除 $ab\,(a,b\in R)$ 的素元 $p\in R$ 一定整除 a 或 b.

证明 设 R 是唯一因子分解整环, 且 $ab=pc$. 如果

$$a=\prod a_i,\ b=\prod b_j,\ c=\prod c_k$$

分别是 a,b,c 到素因子的分解, 则等式 $\prod a_i\times\prod b_j = p\prod c_k$ 意味着, 元素 p 相伴于 a_i 或 b_j 之一, 即 p 整除 a 或 b.

反之: 条件 $p|ab\Rightarrow p|a$ 或 $p|b$ 意味着 R 中因子分解的唯一性. 用归纳法, 假定在 R 中所有满足下述性质的元素是因子分解唯一的, 这种元素存在某个分解式, 式中素因子的个数 $\leqslant n$ (精确到因子的排序和相伴). 现在我们对能够分解成 $n+1$ 个素因子乘积的任意元素 $a\neq 0$ 进行证明. 设

$$a=\prod_{i=1}^{n+1} p_i = \prod_{j=1}^{m+1} r_j \tag{2}$$

是使得 $m\geqslant n$ 的两个分解式. 将定理的条件应用于 $p=p_{n+1}$, 得到 p_{n+1} 应当是 $r_1,\dots,r_{m+1}$ 中某个元素的因子. 不失一般性 (因为可对元素重新标号), 我们认为 $p_{n+1}|r_{m+1}$ 但 r_{m+1} 是素元, 所以 $r_{m+1}=up_{n+1}$, 其中 u 是可逆元. 用 R 中的消去律 (第 4 章 §1 定理 1), 从 (2) 式得到 $\prod\limits_{i=1}^{n} p_i = u\prod\limits_{j=1}^{m} r_j$. 左边是 n 个素元的乘积. 根据归纳假设, $m=n$, 且两个分解精确到素因子的次序以及可逆因子. □

例 1　考察虚二次域 $\mathbb{Q}(\sqrt{-5})$ (见 §1 第 5 段的例子) 中的整环 $R=\{a+b\sqrt{-5}|a,b\in\mathbb{Z}\}$.$R$ 中任意非零元素 $\alpha=a+b\sqrt{-5}$ 的范数 $N(a+b\sqrt{-5})=a^2+5b^2$ 是正整数. 如果 α 在 R 中是可逆的，则 $(N(\alpha))^{-1}=N(\alpha^{-1})\in\mathbb{Z}$，因而 $N(\alpha)=1$. 这仅当 $b=0,a=\pm1$ 时才能发生. 于是像 $\mathbb{Z}$ 中一样， R 中的可逆元只有 ±1. 如果 $\alpha=\varepsilon\alpha_1\alpha_2\ldots\alpha_r\neq0,\varepsilon=\pm1$，则 $N(\alpha)=N(\alpha_1)\ldots N(\alpha_r)$. 因为 $1<N(\alpha_i)\in\mathbb{N}$，所以对于给定的 α，因子的个数 r 是有界的. 于是 R 中的任意元素都有素因子分解.

数 9(不仅是 9) 有两个不同的素因子分解

$$9=3\cdot3=(2+\sqrt{-5})(2-\sqrt{-5}),$$

3 和 $2\pm\sqrt{-5}$ 是不相伴的. 事实上， $N(3)=N(2\pm\sqrt{-5})=9$. 所以从 $\alpha=3$ 或 $2\pm\sqrt{-5}$ 的分解式 $\alpha=\alpha_1\alpha_2$, 其中 α_1,α_2 不可逆，得到 $9=N(\alpha)=N(\alpha_1)N(\alpha_2)$，即 $N(\alpha_i)=3,i=1,2$，这是不可能的，因为方程 $x^2+5y^2=3$ 在 $\mathbb{Z}$ 中无解. 这就证明了元素 3 和 $2\pm\sqrt{-5}$ 是素元.

所考察的例子包含了关于二次域 $\mathbb{Q}\left(\sqrt{d}\right)$ 在萌芽时期的一大类问题，其中的一部分直到现在还没有解决. 这些问题在 *代数数论* 中进行研究.

在利用定理 1 建立其他的唯一因子分解环之前，我们引入一些辅助概念，它们自身亦引起人们的兴趣.

2. 环中的最大公因 (g.c.d.)**和最小公倍**(l.c.m.)　设 R 是一个整环，两个元素 $a,b\in R$ 的 **最大公因** 记作 g.c.d.(a,b)，它是具有如下两条性质的元素 $d\in R$:

i) $d|a,d|b$;

ii) $c|a,c|b\Rightarrow c|d$.

显然， d 的任意相伴元 也满足性质 i),ii). 反之：如果 c 和 d 是元素 a 与 b 的两个最大公因，则 $c|d,d|c$, 于是 c 和 d 是相伴元 . 记号 g.c.d.(a,b) 用于任意最大公因，即在这种写法中，我们对相伴元不加区分. 考虑到将性质 i),ii) 规定为最大公因的定义，可增加下述结论：

iii) g.c.d.$(a,b)=a\Leftrightarrow a|b$;

iv) g.c.d.$(a,0)=a$;

v) g.c.d.$(ta,tb)=t$ g.c.d.(a,b);

vi) g.c.d.(g.c.d.$(a,b),c)=$ g.c.d.$(a,$　g.c.d.$(b,c))$.

验证它们并不困难，留给读者作为练习. 性质 vi) 使得我们可以将最大公因的概念推广到任意有限个元素上. 对于元素 $a,b\in R$, 类比最大公因 g.c.d.(a,b), 可以引出 **最小公倍** l.c.m.(a,b) 的概念，它是由下述两条性质 (精确到相伴) 来定义的：

i′) $a|m,b|m$;

ii′) $a|c,b|c\Rightarrow m|c$.

特别地，令 $c=ab$, 则有 $m|ab$.

定理 2　*设整环 R 中的两个元素 a,b 有最大公因和最小公倍. 则*

a) $\text{l.c.m.}(a,b)=0, \Leftrightarrow a=0$ 或 $b=0$.

b) $a,b\neq 0, m=\text{l.c.m.}(a,b)$, 且 $ab=dm \Rightarrow d=\text{g.c.d.}(a,b)$.

证明 论断 a) 可由 $\text{l.c.m.}(a,b)$ 的定义直接得到. 为了证明论断 b), 我们需要验证由等式 $ab=dm$ 定义的元素 d 满足性质 i), ii). 事实上, i′) $\Rightarrow m=a'a, m=b'b$. 于是 $ab=dm=da'a$, 因为 R 是整环, 消去 a 后得到 $b=da'$, 即 $d|b$. 类似地, $ab=dm=db'b\Rightarrow a=db'$, 即 $d|a$, 我们得到了 i).

其次, 设 $a=fa'', b=fb''$. 令 $c=fa''b''$. 这时 $c=ab''=ba''$ 是 a 和 b 的公倍. 根据性质 ii′), 存在 $c'\in R$, 使 $c=c'm$ 因而 $fc'm=fc=f^2a''b''=ab=dm$, 即 $d=fc'$, 所以 $f|d$. 我们得到了 ii). □

定义 设整环的两个元素 a,b 有最大公因, 如果 $\text{g.c.d.}(a,b)=1$, 则称 a,b 是**互素的**.

从性质 i), ii), i′), ii′) 或定理 2 既不能得出 $\text{g.c.d.}(a,b)$ 和 $\text{l.c.m.}(a,b)$ 的计算方法, 也不能保证它们的存在性. 定理 2, b) 仅建立了它们之间的一个关系.

现在假定 R 是唯一因子分解环. 用 $\mathcal{P}$ 表示 R 中素元的一个集合, 使得 R 中任意的素元相伴且仅相伴于 $\mathcal{P}$ 中的一个元素. 考察两个元素 $a,b\in R$ 的分解时下述约定有时很方便, 即认为它们的因子是取自 $\mathcal{P}$ 的相同元素, 但这时可能出现零指数, 也就是说

$$\begin{gathered} a=up_1^{k_1}\dots p_r^{k_r}, \quad b=vp_1^{l_1}\dots p_r^{l_r}, \\ u|1, \quad v|1, \quad k_i\geqslant 0, \quad l_i\geqslant 0; \quad p_i\in\mathcal{P}; \quad 1\leqslant i\leqslant r. \end{gathered} \tag{3}$$

根据定理 1, 得到下述便于记忆的

整除性判别法 设 R 是唯一因子分解整环; a,b 是环 R 的两个元素, 分别表示成 (3) 式的形式.

则下述论断成立:

1) $a|b$ 当且仅当 $k_i\leqslant l_i, \quad i=1,2,\cdots,r$;

2) $\text{g.c.d.}(a,b)=p_1^{s_1}\cdots p_r^{s_r}$, 其中 $s_i=\min\{k_i,l_i\}, i=1,2,\cdots,r$;

3) $\text{l.c.m.}(a,b)=p_1^{t_1}\cdots p_r^{t_r}$, 其中 $t_i=\max\{k_i,l_i\}, i=1,2,\cdots,r$.

这样 s_i 需要取两个指数 k_i,l_i 中最小的, 而 t_i 取最大的. 特别地, 元素 $a,b\in R$ 互素, 当且仅当出现在一个元素分解式中的素因子, 不出现在另一个元素的分解式中.

这个整除性判别法的缺陷在于, 得到形如 (3) 的分解式实际上是非常困难的. 即使在 $R=\mathbb{Z}$ 的情况下 (此处不预先假定 $\mathbb{Z}$ 的唯一因子分解性), 人们也只能对给定整数 n, 直接挑选所有小于 n 的素数这一方式作些意义不大的改动. 下面将要给出在一类环中计算 g.c.d. 和 l.c.m. 的有效方法, 这是令人愉快的.

3. 欧几里得环的唯一因子分解性 在 $\mathbb{Z}$ 和 $P[X]$ 中的带余除法 (见第 1 章的 §9 第 3 段和 §2 第 3 段), 使我们自然地想到去考察一类整环 R, 其中每个元素 $a\neq 0$

对应于一个非负整数 $\delta(a)$, 也就是说存在一个映射

$$\delta: R\backslash\{0\} = R^* \to \mathbb{N} \cup \{0\},$$

满足如下条件:

E1) $\delta(ab) \geqslant \delta(a)$对任意 R 的元素 $a, b \neq 0$ 成立;

E2) 任取 $a, b \in R, b \neq 0$, 存在 $q, r \in R$(q 叫作"商"元, r 叫作"余"元), 使得

$$a = qb + r; \quad \delta(r) < \delta(b)\text{或 } r = 0. \tag{4}$$

满足这一性质的整环 R 叫作 **欧几里得环**(简称 **欧氏环**). 若 $a \in \mathbb{Z}$, 令 $\delta(a) = |a|$, 若 $a = a(X) \in P[X]$, 令 $\delta(a) = \deg a$, 我们看到 $\mathbb{Z}$ 和 $P[X]$ 是欧氏环.

在欧氏环中有一种计算 g.c.d.(a, b) 的方法, 叫作 **辗转相除法** 或 **欧几里得算法**, 可作如下解释. 设给定欧氏环 R 中的非零元素 a, b, 足够多 (但是有限) 次地运用 E2), 我们得到了一组形如 (4) 的等式, 最后一个式子的余元素为零:

$$\begin{array}{ll} a = q_1 b + r_1, & \delta(r_1) < \delta(b), \\ b = q_2 r_1 + r_2, & \delta(r_2) < \delta(r_1), \\ r_1 = q_3 r_2 + r_3, & \delta(r_3) < \delta(r_2), \\ \cdots\cdots\cdots\cdots & \\ r_{k-2} = q_k r_{k-1} + r_k, & \delta(r_k) < \delta(r_{k-1}), \\ r_{k-1} = q_{k+1} r_k, & r_{k+1} = 0. \end{array} \tag{5}$$

事实上, 因为非负整数的严格递减数列 $\delta(b) > \delta(r_1) > \delta(r_2) > \cdots$ 必然中断, 而中断点仅可能当余元素为零时出现.

我们断言, 最后一个非零余元素 r_k 就是在第 2 段定义的元素 a 和 b 的最大公因. 事实上, 根据条件, $r_k | r_{k-1}$. 在等式组 (5) 中自下而上, 并运用在第 1 段给出的关于整除的性质 (4), 得到一系列整除关系 $r_k | r_{k-1}, r_k | r_{k-2}, \cdots, r_k | r_2, r_k | r_1$, 最后, $r_k | b, r_k | a$. 于是 r_k 是元素 a, b 的公因子. 反之, 设 c 是 a, b 的任意一个公因子, 则 $c | r_1$, 现在在等式组 (5) 中自上而下, 得到了一系列整除关系 $c | r_2, c | r_3, \cdots, c | r_k$. 由此可最后断定, g.c.d.$(a, b)$ 存在, 且等于 r_k:

$$r_k = \text{g.c.d.}(a, b). \tag{6}$$

其次注意到, 当 $i \geqslant 3$ 时, 等式组 (5) 中的每一个余元素 r_i 都可以表示成系数在 R 中的前两个余元素 r_{i-1} 和 r_{i-2} 的线性组合. r_1 可以通过 a 和 b 表示: $r_1 = a - q_1 b$, 而 r_2 通过 b 和 r_1 表示, 它仍然是 a 和 b 的线性组合. 顺次在 r_i 中用 a, b 的表达式置换 r_{i-1}, r_{i-2}, 我们得到 $i = k$ 时的表达式

$$r_k = au + bv \tag{7}$$

其中元素 $u, v \in R$.

比较 (6) 和 (7) 并注意到定理 2, b), 我们得到下述论断.

定理 3 在欧氏环 R 中, 任意两个元素 a, b 都有最大公因和最小公倍. 利用欧几里得算法, 可以找到元素 $u, v \in R$, 使得

$$\text{g.c.d.}(a, b) = au + bv.$$

特别地, 元素 a, b 互素, 当且仅当存在元素 $u, v \in R$, 使得

$$au + bv = 1.$$

推论 设 a, b, c 是欧氏环 R 中的元素.

i) 如果 $\text{g.c.d.}(a, b)=1$ 且 $\text{g.c.d.}(a, c)=1$, 则 $\text{g.c.d.}(a, bc)=1$.

ii) 如果 $a \big| bc$ 且 $\text{g.c.d.}(a, b)=1$ 则 $a \big| c$.

iii) 如果 $b \big| c, a \big| c$, 且 $\text{g.c.d.}(b, c)=1$, 则 $bc \big| a$.

证明 i) 根据定理 3 有等式 $au_1 + bv_1 = 1, au_2 + cv_2 = 1$. 将它们的左右两端分别相乘, 我们得到 $a(au_1u_2 + bu_2v_1 + cu_1v_2) + bc(v_1v_2) = 1$, 结论得证.

ii) 我们有 $au + bv = 1$, 从而 $ac \cdot u + (bc)v = c$. 但 $bc = aw$, 所以 $c = a(cu + wv)$, 即 $a \big| c$.

iii) 根据最小公倍的性质 ii′),

$$b \big| a, c \big| a \Rightarrow \text{l.c.m.}(b, c) \big| a \Rightarrow bc \big| a,$$

这是因为 $bc = \text{g.c.d.}(b, c) \cdot \text{l.c.m.}(b, c)$, 而根据条件, $\text{g.c.d.}(b, c) = 1$. □

读者不难将定理 3 推广到欧氏环中任意有限多个元素的情况.

证明欧氏环的唯一因子分解性质的第一步是下述引理.

引理 欧氏环 R 是有因子分解的环 (即 R 中的任意元素 $a \neq 0$ 可以写成 (1) 式的形式).

证明 设元素 $a \in R$ 有真因子 b: $a = bc$, 此处 b 和 c 都不是可逆元 (换言之, a 和 b 不相伴). 我们来证明 $\delta(b) < \delta(a)$.

事实上, 根据 E1) 直接得到 $\delta(b) \leqslant \delta(bc) = \delta(a)$. 假设等式成立 $\delta(b) = \delta(a)$, 利用条件 E2) 可以找到 q, r, 使 $b = qa + r$, 其中 $\delta(r) < \delta(a)$ 或 $r = 0$.$r = 0$ 的情况与 a 和 b 不相伴矛盾. 其次, 因为 c 不是可逆元, $1 - qc \neq 0$. 再次根据 E1)(将 a 换成 b) 有

$$\delta(a) = \delta(b) \leqslant \delta(b(1 - qc)) = \delta(b - qa) = \delta(r) < \delta(a),$$

得到矛盾. 于是 $\delta(b) < \delta(a)$.

现在若 $a = a_1a_2 \cdots a_n$, 其中所有的 a_i 都是不可逆的, 则 $a_{m+1}a_{m+2} \cdots a_n$ 是 $a_ma_{m+1} \cdots a_n$ 的真因子, 根据上述证明

$$\delta(a) = \delta(a_1a_2 \cdots a_n) > \delta(a_2 \cdots a_n) > \cdots > \delta(a_n) > \delta(1).$$

这个严格递减非负整数列的长度 $n \leqslant \delta(a)$. 所以对于元素 $a \in R$, 有一个长度最大的分解, 它就是 a 的素因子分解. □

定理 4 *每一个欧氏环都是唯一因子分解整环.*

证明 利用上述引理和定理 1 给出的唯一因子分解判别准则, 我们只需证明, 如果 p 是环 R 中能够整除乘积 bc 的一个素元, 其中 $b, c \in R$, 则 $p|b$ 或 $p|c$.

事实上, 当 $b=0$ 或 $c=0$ 时, 无需证明. 如果 $bc \neq 0$, 且 $d = \text{g.d.c.}(b,p)$, 则 d 是素元 p 的因子, 它或为 1(准确地说, 是 1 的因子) 或与 p 相伴. 在第一种情况下, b 和 p 是互素的, 定理 3 的推论 ii) 表明 $p|c$. 在第二种情况下, $d = up, u|1$, 意味着 $p|b$. □

推论 环 $\mathbb{Z}$ 和 $P[X]$ (P 是任意一个域) 是唯一因子分解整环.

证明 直接由欧氏环的定义, 对 $\mathbb{Z}$ 和 $P[X]$ 自然地定义具有性质 E1),E2) 的函数 δ, 再运用定理 4. □

建议对 $\mathbb{Z}$ 和 $P[X]$ 因子分解唯一性的证明分开进行, 以消除在这一问题上可能出现的任何似是而非的观点.

多元多项式环 $P[X_1, \cdots, X_n], n > 1$, 不是欧氏环, 它的唯一因子分解性将在 [BAⅢ] 中证明. 我们还会给出欧氏环的其他的例子.

4. 既约多项式 再次强调以前的专用定义, 环 $P[X]$ 的一个次数大于零的多项式 f 叫作既约的, 如果 f 不被任何多项式 $g \in P[X]$ 整除, 其中 $0 < \deg g < \deg f$. 特别地, 所有的一次多项式都是既约的. 显然, 次数大于 1 的多项式的既约性 (或它到既约因子的分解) 是一个与基域 P 密切相关的概念, 例如, 我们已经知道, 根据复数的构造, 多项式 $X^2+1=(X+i)(X-i)$. 域 $\mathbb{Q}$ 上的多项式 X^4+4 是可约的, 尽管不易猜到:

$$X^4+4=(X^2-2X+2)(X^2+2X+2).$$

右边的两个多项式不仅在 $\mathbb{Q}$ 上, 而且在 $\mathbb{R}$ 上都是不可约的, 但在 $\mathbb{C}$ 上是可约的.

正如素数在 $\mathbb{Z}$ 中有无穷多个一样 (见第 1 章 §1),*任意域上的首一既约多项式也有无穷多个.*

在无限域 P 的情况下, 这是显然的: 考察形如 $X-c, c \in P$ 的既约多项式即可.

如果域 P 是有限的, 应用欧几里得的论证. 设我们已经找到 $P[X]$ 中的全部 n 个首一既约多项式 $p_1, \cdots, p_n$. 则多项式 $f = p_1p_2\cdots p_n+1$ 至少有一个首一素因子, 这是因为 $\deg f \geqslant n$. 将它记作 p_{n+1}. 它与 $p_1, \cdots, p_n$ 都不相同, 否则若存在 $s \leqslant n$, 使得 $p_{n+1}=p_s$, 则 $p_s|(f-p_1\cdots p_n)$, 即 $p_s|1$, 得到矛盾. □

由于有限域上指定次数的多项式只有有限多个, 我们得到下述有用的结论.

在任意有限域上, 存在任意高次的既约多项式.

这一定性的论断将在 [BAⅢ] 中精确地阐述.

域 $\mathbb{Q}$ 上的既约多项式在代数数域理论中起着特殊的作用. 因为用一个适当的自

然数去乘 $\mathbb{Q}[X]$ 中的多项式总可以得到 $\mathbb{Z}[X]$ 中的多项式，所以先要弄清楚 $\mathbb{Q}$ 上多项式的既约性与 $\mathbb{Z}$ 上多项式既约性之间的关系. 因为对其他方面的应用也感兴趣，我们先来证明一个有关唯一因子分解环 R 上的多项式的一般论断.

多项式 $f = a_0 + a_1X + \cdots + a_nX^n \in R[X]$ 的所有系数的最大公因 $d = d(f)$ 叫作 f 的 **容度**. 到目前为止，我们只讨论了两个元素的最大公因 g.c.d.(a, b), 但最大公因的性质 i)—vi) 允许我们将这一概念推广到整环中的任意有限多个元素上去.

如果 $d(f)$ 是 R 中的可逆元，则多项式 f 叫作 **本原多项式**.

高斯引理　*设 R 是一个唯一因子分解环，$f, g \in R[X]$. 则*

$$d(fg) \approx d(f) \cdot d(g)$$

(其中 $\approx$ 指精确到相伴是相等的). 特别地，任意两个本原多项式的乘积仍然是本原多项式.

证明　从后一个断言开始证明. 假设

$$f = a_0 + a_1X + \cdots + a_nX^n, \quad g = b_0 + b_1X + \cdots + b_mX^m$$

是 $R[X]$ 中的两个本原多项式，而乘积 fg 不是本原的. 于是存在素元 $p \in R$, 能够除尽 $d(fg)$. 选择最小的下标 s, t, 使得 $p \nmid a_s, p \nmid b_t$. 这样的下标可以找到，因为 f 和 g 都是本原的. X^{s+t} 在 fg 中的系数是

$$c_{s+t} = a_sb_t + (a_{s+1}b_{t-1} + a_{s+2}b_{t-2} + \cdots) + (a_{s-1}b_{t+1} + a_{s-2}b_{t+2} + \cdots).$$

根据假设条件，a_{s-i} 和 b_{t-i} 当 $i > 0$ 时被 p 整除，且 $p|c_{s+t}$, 我们有关系式

$$pu = a_sb_t + pv,$$

所以 $p|a_sb_t$. 由 R 的唯一因子分解性得到 $p|a_s$ 或 $p|b_t$，引出矛盾，这就证明了我们的论断.

进入一般情况，将任意多项式 $f, g \in R[X]$ 写成形式

$$f = d(f)f_0, \quad g = d(g)g_0,$$

其中 f_0, g_0 是本原多项式. 因为 $fg = d(f)d(g) \cdot f_0g_0$, 而且我们已经证明了 $d(f_0g_0) \approx 1$, 故 $d(fg) \approx d(f)d(g)$. □

推论　*设多项式 $f \in \mathbb{Z}[X]$，若 f 在 $\mathbb{Z}$ 上是既约的，则在 $\mathbb{Q}$ 上也是既约的.*

证明　根据定理 4 的推论，$\mathbb{Z}$ 是唯一因子分解整环，所以可以对 $\mathbb{Z}[X]$ 应用高斯引理. 假定 $f = gh$, 其中 $f \in \mathbb{Z}[X]$，而 $g, h \in \mathbb{Q}[X]$. 在等式两端同乘 g 和 h 的所有系数的分母的最小公倍，等式变为 $af = bg_0h_0$, 其中 $a, b \in \mathbb{Z}$，而 g_0, h_0 是 $\mathbb{Z}$ 上的本原多项式. 根据高斯引理，$a \cdot d(f) = b$(不失一般性，可以在等式中代之以相伴元), 于是得到了 $\mathbb{Z}$ 上的因式分解 $f = d(f)g_0h_0$, 与 f 在 $\mathbb{Z}[X]$ 中的既约性矛盾. □

艾森斯坦既约性判别法 设

$$f(X) = X^n + a_1X^{n-1} + \cdots + a_{n-1}X + a_n$$

是 $\mathbb{Z}$ 上的首一多项式，如果所有的系数 $a_1, \cdots, a_n$ 都能够被某个素数 p 整除，但 a_n 不能被 p^2 整除．则 $f(X)$ 在 $\mathbb{Q}$ 上是既约的．

证明 假设 $f(X)$ 在 $\mathbb{Q}$ 上可约，利用高斯引理，可以将 $f(X)$ 写成 $\mathbb{Z}$ 上两个首一多项式的乘积:

$$f(X) = (X^s + b_1X^{s-1} + \cdots + b_s)(X^t + c_1X^{t-1} + \cdots + c_t), s, t > 0.$$

这个分解式在 $\mathbb{Z}_p[X]$ 中仍然成立，它由整系数多项式对系数取模 p 的剩余类得到．根据条件 $\overline{a_i} = \bar{0}$，其中 $\overline{a_i}$ 是整数 a_i 模 p 的剩余类．但 $\mathbb{Z}_p[X]$ 是唯一因子分解环 (定理 4 的推论)．比较两个分解式:

$$X^sX^t = (X^s + \overline{b}_1X^{s-1} + \cdots)(X^t + \overline{c_1}X^{t-1} + \cdots), s + t = n,$$

我们得到结论 $\overline{b_i} = \bar{0} = \overline{c_j}$，即所有的系数 b_i, c_j 都可以被 p 整除，在这种情况下，$a_n = b_sc_t$ 被 p^2 整除，得到矛盾，艾森斯坦判别法得证． □

注意 当首项系数不等于 1 但与 p 互素时，判别法仍然可用．

例 2 任取素数 p，多项式 $f(X) = X^{p-1} + X^{p-2} + \cdots + X + 1$ 在 $\mathbb{Q}$ 上是既约的．

只要注意到 $f(X)$ 的既约性等价于多项式

$$f(X+1) = \frac{(X+1)^p - 1}{(X+1) - 1} = X^{p-1} + \binom{p}{1}X^{p-2} + \cdots + \binom{p}{p-2}X + \binom{p}{p-1}$$

的既约性，后者除首项系数外，所有的系数均可被 p 的一次幂整除 (二项系数的性质，见第 4 章 §3 习题 6)，对这个多项式应用艾森斯坦判别法．

习　　题

1. 证明

$$n\mathbb{Z} + m\mathbb{Z} = \mathbb{Z} \cdot \text{g.c.d.}(n, m),$$
$$n\mathbb{Z} \cap m\mathbb{Z} = \mathbb{Z} \cdot \text{l.c.m.}(n, m).$$

2. 设 f 和 g 是 $\mathbb{Z}[X]$ 中的首一多项式，证明在等式 $\text{g.c.d.}(f, g) = fu + gv$ 中，其中 $u, v \in \mathbb{Z}[X]$，可以使得 $\deg u < \deg g, \deg v < \deg f$.

3. 环 $\mathbb{Z}[\sqrt{-3}]$ 和 $\mathbb{Z}_8[X]$ 是唯一因子分解环吗？

4. 当 $5 \leqslant n \leqslant 12$ 时，将 $\mathbb{Z}[X]$ 中的多项式 $X^n - 1$ 分解成素因式的乘积．

5. 证明齐次多项式

$$f(X, Y) = a_0X^n + a_1X^{n-1}Y + \cdots + a_{n-1}XY^{n-1} + a_nY^n \in \mathbb{Q}[X, Y]$$

的既约因式也是齐次的，并且 $f(X,Y)$ 是既约的，当且仅当 $f(X,1)=a_0X^n+a_1X^{n-1}+\cdots+a_{n-1}X+a_n\in\mathbb{Q}[X]$ 是既约的.

6. 设 P 是一个域，$f(X)=\sum_{i\geqslant 0}a_iX^i$ 是 $P[[X]]$ 中的形式幂级数（见 §2 习题 5），条件 $a_0\neq 0$，或等价地 $\omega(f)=0$，是存在幂级数 $g\in P[[X]]$，使得 $fg=1$ 的充分必要条件. 例如，$(1-X)^{-1}=\sum_{i\geqslant 0}X^i$. 精确到相伴，$X$ 是 $P[[X]]$ 中唯一的素元. 环 $P[[X]]$ 是唯一因子分解整环. 证明这三个论断.

7. 证明 $\det(X_{ij})=\sum_{\pi\in S_n}\varepsilon_\pi x_{\pi(1),1}\cdots x_{\pi(n),n}$ 是 n^2 个变元 x_{ij} 的 n 次齐次既约多项式.

提示：假定情况相反，令

$$\det(x_{ij})=g_1(\cdots,x_{ij},\cdots)g_2(\cdots,x_{ij},\cdots).$$

因为 $\det(x_{ij})$ 是变元取自某个固定列的线性齐次多项式，因而因式 g_1,g_2 之一是 x_{ij} 的线性齐次多项式，其中 $1\leqslant i\leqslant n,j$ 是固定的，同时另一个因子不依赖于这些 $x_{ij},1\leqslant i\leqslant n$. 当把列换成行时，类似的结论仍然成立. 现在设 x_{11} 出现在 g_1 中. 则 g_2 不包含有 $x_{1j},1\leqslant j\leqslant n$，从而 g_2 不包含有 $x_{ij},1\leqslant i,j\leqslant n$，即 g_2 是一个常数.

§4 分式域

1. 整环的分式域的构造 在前面两节中建立了 $\mathbb{Z}$ 和 $P[X]$ 许多共有的性质. 我们的下一个目标是将 $P[X]$ 嵌入到一个域中，并且只需最简便方法做到这点，就像将 $\mathbb{Z}$ 嵌入到 $\mathbb{Q}$ 中一样. 事实上，对任何整环 A 解决这样的问题都不复杂.

考察所有的元素对 (a,b),$a,b\in A,b\neq 0$ 组成的集合 $A\times A^*(A^*=A\setminus\{0\})$. 我们将这一集合划分为类，两个元素对 (a,b) 和 (c,d) 在同一类中，若 $ad=bc$，记作：$(a,b)\sim(c,d)$. 显然 $(a,b)\sim(a,b)$ 永远成立. 其次 $(a,b)\sim(c,d)\Leftrightarrow(c,d)\sim(a,b)$，最后 $(a,b)\sim(c,d),(c,d)\sim(e,f)\Rightarrow(a,b)\sim(e,f)$. 事实上，由等式 $ad=bc,cf=de$ 得到 $adf=bcf=bde$，即 $d(af-be)=0$. 但 $d\neq 0$，根据环 A 的整性，得到 $af=be$，即 $(a,b)\sim(e,f)$. 于是，关系 $\sim$ 是反身、对称、传递的，也就是说（见第 1 章 §6），它是一个定义于集合 $A\times A^*$ 上的等价关系，从而把 $A\times A^*$ 划分成不相交的类.

设 $Q(A)$ 是所有等价类的集合，或 $Q(A)$ 是集合 $A\times A^*$ 关于等价关系的商集 $A\times A^*/\sim$. 用符号 $[a,b]$ 表示有序对 (a,b) 所在的类. 根据定义

$$[a,b]=[c,d]\Leftrightarrow ad=bc \tag{1}$$

如果在集合 $A\times A^*$ 上用下述公式给出加法和乘法运算

$$(a,b)+(c,d)=(ad+bc,bd),\quad (a,b)(c,d)=(ac,bd)$$

（因为在 A 中，从 $b\neq 0,d\neq 0$ 可以推出 $bd\neq 0$，这样做是有意义的），这些二元运算也

可以转移到 $Q(A)$ 上. 事实上, 我们需要指出,

$$(a',b')\sim(a,b)\Rightarrow\begin{cases}(a,b)+(c,d)\sim(a',b')+(c,d),\\(a,b)(c,d)\sim(a',b')(c,d).\end{cases}$$

这件事可表达为关系式

$$(ad+bc)b'd=(a'd+b'c)bd,$$

$$ac\cdot b'd=a'c\cdot bd$$

的正确性, 后者从条件 $a'b=ab'$ 直接得到. 如果 $cd'=c'd$, 则将 (c,d) 换成 (c',d') 时, 类似的结果成立. 我们断言, $Q(A)$ 上的加法与乘法运算不依赖于等价类中代表元的选取, 于是我们有

$$[a,b]+[c,d]=[ad+bc,bd],[a,b][c,d]=[ac,bd]. \tag{2}$$

此处本应记作比如 $[a,b]\oplus[c,d]$ 和 $[a,b]\odot[c,d]$, 但 $\oplus$ 和 $\odot$ 仍采用通常的加法和乘法记号时, 并未失去表述的清晰性.

现在我们来证明在 (2) 定义的运算下, $Q(A)$ 是一个域. 首先, 关系式

$$[a,b]+([c,d]+[e,f])=[a,b]+[cf+de,df]=[adf+bcf+bde,bdf],$$
$$([a,b]+[c,d])+[e,f]=[ad+bc,bd]+[e,f]=[adf+bcf+bde,bdf]$$

保证了加法运算的结合律. 乘法满足结合律是显然的. 其次, 关系式

$$([a,b]+[c,d])\cdot[e,f]=[ade+bce,bdf],$$
$$[a,b][e,f]+[c,d][e,f]=[adef+bcef,bfdf]=[(ade+bce)f,(bdf)f]$$

和等价类相等的条件 (1) 表明, 分配律成立.

加法和乘法交换律的验证不难. 加法的零元是类 $[0,1]$, $([0,1]+[a,b]=[a,b])$, 而乘法的单位元是类 $[1,1]$. 其次, $-[a,b]=[-a,b]$, 因为 $[a,b]+[-a,b]=[0,b^2]=[0,1]$. 上述所有的条件表明, $Q(A)$ 是一个有单位元的交换环. 如果 $[a,b]\neq[0,1]$, 则在 A 中 $a\neq 0$, 故 $[b,a]\in Q(A)$, 且 $[a,b]\cdot[b,a]=[1,1]$, 于是当 $[a,b]\neq[0,1]$ 时, 其乘法逆元为 $[b,a]$. 从而 $Q(A)$ 是一个域.

定义一个映射 $f\colon A\to Q(A), a\mapsto[a,1]$, 则 f 是一个环的单同态 (事实上 $f(a+b)=f(a)+f(b), f(ab)=f(a)f(b)$; $a\neq b\Rightarrow f(a)\neq f(b)$) . 任取元素 $x=[a,b]\in Q(A)$, 我们有

$$[b,1]x=[a,1],$$

于是 x 是 $f(A)$ 中元素的 "比" $f(a)/f(b)$. 由于这个原因, $Q(A)$ 叫作**环 A 的分式域**.

为方便起见，我们将元素 $a \in A$ 与它的像 $f(a)=[a,1]\in Q(A)$ 等同起来，即将 A 与 $f(A)$ 等同起来. 于是可以把每一个元素 $[a,1]\in Q(A)$ 换成 $a\in A$, 保留域 $Q(A)$ 中所有其他的元素不变，比如在公式 (2) 中发生如下改变：

$$a+[b,c]=[ac+b,c], a[b,c]=[ab,c].$$

归根到底，整环 A 从一开始就是与 $Q(A)$ 同构并能体现出 $Q(A)$ 这一符号的通常意义的某个域的子环. 经过这样的恒同之后，我们就可以合理地称元素 $[a,b]$ 为 **分式**, 并按照习惯简记作下述形式：

$$[a,b]=\frac{a}{b}.$$

不难想到，类 $[a,b]$ 的运算法则与域中分式的运算法则 (见第 4 章 §3 第 4 段中的 (8) 式) 是一致的. 我们证明了

定理 1　*对于任意一个整环 A, 存在一个分式域 $Q(A)$, 它的元素形如 a/b, $a\in A, 0\neq b\in A$. 运算由法则 (1),(2) 给出，其中 $[a,b]=a/b$.*　□

分式域的构造在数学中经常使用. 域 $\mathbb{Q}$ 是环 $\mathbb{Z}$ 的分式域 $Q(\mathbb{Z})$ 表明，这是一个很自然的想法. 易见，当 A 是域时， $Q(A)\cong A$ (验证这一点).

注记　可以证明，若整环 A 是域 P 的一个子环，且每个元素 $x\in P$ 能够写成比的形式 a/b, 其中元素 $a\in A, 0\neq b\in A$, 则 $P\cong Q(A)$. 例如 $\mathbb{Q}(\sqrt{d})=Q(\mathbb{Z}[\sqrt{d}])$.

2. 有理函数域　设 P 是一个域， $P[X]$ 是 P 上的多项式环， $P[X]$ 的分式域记作 $P(X)$ (用圆括号代替方括号), 叫作变元 X 的系数在 P 中的 **有理函数域**.

注意到有理函数域 $P(X)$ 永远包含无限多个元素，它的特征与域 P 的特征一致. 域 $\mathbb{F}_p(X)$ 提供了一个特征为 $p>0$ 的无限域的例子.

域 $P(X)$ 中的每一个有理函数都可以写成 (并且以多种方式写成)f/g 的形式 (或 $\dfrac{f}{g}$, 如果不打算节省篇幅), 其中 f,g 是环 $P[X]$ 中的多项式， $g\neq 0$. 根据定义，$f/g=f_1/g_1 \Leftrightarrow fg_1=f_1g$. 自然地称 f 为有理函数 f/g 的 **分子**, 而称 g 为 **分母**. 当分子分母同乘以同一个非零多项式或消去同一个公因式时，有理函数不变. 特别地，整数 (正，零或负) $\deg f-\deg g$ 不依赖于非零有理函数 f/g 写成两个多项式 f 和 g 的比时代表元的选择. 这个数叫作 **有理函数的次数**. 变元 X 的一个有理函数称为 **既约分式**, 如果它的分子与分母互素. 精确到 P 中元素的分子与分母的公因的乘积，任意有理函数可唯一地表成既约分式. 事实上，用 g.c.d.(f,g) 去除 f 和 g, 就得到一个既约分式，如果两个既约分式 $f/g=f_1/g_1$, 则 $fg_1=f_1g$, 给出 $f=cf_1, g=cg_1, c\in P$(利用 §3 定理 4 的推论).

如果 $\deg(f/g)=\deg f-\deg g<0$, 则 (既约) 分式 f/g 叫作 **真分式**(零多项式也可看作是真分式，因为我们约定 $\deg 0=-\infty$).

定理 2　*$P(X)$ 中的每一个有理函数都可以唯一地表成一个多项式与一个真分式的和.*

证明 对有理函数 f/g 的分子和分母使用带余除法，给出等式 $f = qg + r$，其中 $\deg r < \deg g$. 现在 $f/g = q + r/g$ 是所求的写法. 如果还有其他写法 $f/g = \overline{q} + \overline{r}/\overline{g}$ ($\overline{q}, \overline{r}, \overline{g} \in P[X], \deg \overline{r} < \deg \overline{g}$)，则

$$\overline{q} - q = \frac{r}{g} - \frac{\overline{r}}{\overline{g}} = \frac{r\overline{g} - \overline{r}g}{g\overline{g}}.$$

因为 $\overline{q} - q \in P[X]$，而

$$\deg\left(\frac{r\overline{g} - \overline{r}g}{g\overline{g}}\right) = \deg(r\overline{g} - \overline{r}g) - \deg g - \deg \overline{g} < 0,$$

故这种情况仅当 $\overline{q} - q = 0$ 且 $r/g = \overline{r}/\overline{g}$ 时才有可能发生. □

注记 所有真分式的集合 $P_0(X)$ 连同 $P(X)$ 中的加法和乘法运算构成一个没有单位元的环.

事实上，设 $f_1/g_1, f_2/g_2 \in P_0(X)$，因为

$$\deg f_1 f_2 = \deg f_1 + \deg f_2 < \deg g_1 + \deg g_2 = \deg g_1 g_2,$$

故

$$\left(\frac{f_1}{g_1}\right)\left(\frac{f_2}{g_2}\right) = \frac{f_1 f_2}{g_1 g_2} \in P_0(X).$$

其次，

$$\frac{f_1}{g_1} \pm \frac{f_2}{g_2} = \frac{f_1 g_2 \pm f_2 g_1}{g_1 g_2} \in P_0(X),$$

因为每一项 $f_1 g_2$ 和 $f_2 g_1$ 的次数严格小于分母 $g_1 g_2$ 的次数. 我们在定理 2 前的约定使得 $0 \in P_0(X)$，但同时 $1 \notin P_0(X)$. □

到目前为止，我们总是着重于考虑环 $\mathbb{Z}$ 和 $P[X]$ 相似到什么程度. 当转入它们的分式域时，情况发生了本质的变化：与 $P_0(X)$ 不同，$\mathbb{Q}$ 中的真分数不构成环. 例如，

$$\frac{2}{3} + \frac{3}{5} = \frac{19}{15}.$$

3. 最简分式 一个真分式 $f/g \in P(X)$ 叫作 **最简的**，如果 $g = p^n, n \geqslant 1$，其中 $p = p(X)$ 是一个既约多项式，并且 $\deg f < \deg p$.

关于有理函数的基本定理是

定理 3 *每一个真分式都可以唯一地表示成最简分式的和.*

证明 设 $f/g \in P(X)$ 是给定的真分式，不失一般性，可以认为多项式 g 是首一的 (如果 $\lambda \neq 0$ 是 g 的首项系数，则 f/g 等于分式 $\lambda^{-1}f/\lambda^{-1}g$). 下面的讨论分成若干步骤.

步骤 1 令 $g = g_1 g_2$ 是两个互素的首一多项式之积. 则

$$\frac{f}{g_1 g_2} = \frac{f_1}{g_1} + \frac{f_2}{g_2}, \tag{3}$$

右边的两个分式是真分式，并且写法是唯一的. 事实上，从 g_1,g_2 互素得到 (§3 定理 3),$1 = u_1g_1 + u_2g_2$,$u_1,u_2 \in P[X]$. 用 f 去乘等式的两端，我们有 $f = fu_1g_1 + fu_2g_2$. 如果 $fu_2 = qg_1 + f_1$, $\deg f_1 < \deg g_1$(用 g_1 去除 fu_2 的带余除法), 则 $f = f_1g_2 + f_2g_1$, 其中 $f_2 = fu_1 + qg_2$. 用 g_1g_2 去除等式的两边，即考察以 g_1g_2 为分母的分式，我们得到了所需的表达式 (3), 根据构造， $f_1/g_1 \in P_0(X)$(真分式的集合), 并由第 2 段最后的注记 $f_2/g_2 = f/g - f_1/g_1 \in P_0(X)$.

现在设 $f/g = f_1'/g_1 + f_2'/g_2$ 是与 (3) 式同样类型的真分式的和. 则由等式 $f_1/g_1 + f_2/g_2 = f_1'/g_1 + f_2'/g_2$ 得到

$$(f_1 - f_1')g_2 = (f_2' - f_2)g_1.$$

$(f_1 - f_1')g_2$ 被 g_1 整除, 而 g_1 与 g_2 互素, 所以 $f_1 - f_1'$ 被 g_1 整除. 但 $\deg(f_1 - f_1') < \deg g_1$, 故 $f_1 - f_1' = 0$. 表达式 (3) 是唯一的.

步骤 2 设在真分式 f/g 中，对于 (首一的) 分母 g 有标准分解

$$g = p_1^{n_1} p_2^{n_2} \cdots p_m^{n_m}, \tag{4}$$

其中 $p_1(X),p_2(X),\cdots,p_m(X)$ 是 P 上两两不同的首一既约多项式. 则存在唯一确定的表达式

$$\frac{f}{g} = \sum_{i=1}^{m} f_i/p_i^{n_i},$$

其中 $f_i/p_i^{n_i}$ 是真分式 (这个分式也叫作 **准素分式**).

我们的论断容易根据步骤 1 对 m 作归纳得到：

$$\frac{f}{g} = \frac{f_1}{p_1^{n_1}} + \frac{f_0}{p_2^{n_2} \cdots p_m^{n_m}} = \frac{f_1}{p_1^{n_1}} + \left(\frac{f_2}{p_2^{n_2}} + \cdots + \frac{f_m}{p_m^{n_m}}\right).$$

因为 f_1 和 f_0 是唯一确定的，由归纳假设， $f_2,\cdots,f_m$ 也是唯一确定的.

步骤 3 所有的真准素分式 a/p^n 都可以唯一地表示成最简分式的和.

事实上，根据条件， $\deg a < n \deg p$, 欧几里得带余除法给出了一系列的等式

$$a = q_1p^{n-1} + r_1, \deg r_1 < (n-1)\deg p,$$

$$r_1 = q_2p^{n-2} + r_2, \deg r_2 < (n-2)\deg p,$$

$$\cdots\cdots\cdots\cdots$$

$$r_{n-2} = q_{n-1}p + r_{n-1}, \deg r_{n-1} < \deg p,$$

$$r_{n-1} = q_n,$$

其中 $\deg q_i < \deg p$ 对所有唯一确定的 $q_1,\cdots,q_n$ 成立. 我们看到

$$a = q_1p^{n-1} + q_2p^{n-2} + \cdots + q_{n-1}p + q_n,$$

因而

$$\frac{a}{p^n}=\frac{q_1}{p}+\frac{q_2}{p^2}+\cdots+\frac{q_{n-1}}{p^{n-1}}+\frac{q_n}{p^n}.$$

因为 $\deg q_i<\deg p$, 分式 q_i/p^i 是最简的. 根据构造，它们是唯一确定的 (类似于将整数分解为 2 进小数，或类似于十进小数).

步骤 4 将 1~3 的结论综合到一起，定理得证. □

从定理 3 的证明可见，如果 f/g 是真分式，那么由 g 的标准分解 (4) 给出最简分式的分母是 $p_1^{n_1},p_1^{n_1-1},\cdots,p_1;\cdots;p_m^{n_m},p_m^{n_m-1},\cdots,p_m$.

最简分式本身对于代数不是迫切需要的 (即使给出环的新例子), 但在分析中地位重要. 这是由域 $\mathbb{C}$ 和 $\mathbb{R}$ 上既约多项式的特殊形状决定的，关于这一点将在第 6 章中详细讨论.

习 题

1. 构造系数取自实数域 $\mathbb{R}$ 上单变元 X 的形式幂级数环 $\mathbb{R}[[X]]$ 的分式域 $\mathbb{R}((X))$. 根据 §3 习题 6 证明，$\mathbb{R}((X))$ 中的元素形如

$$\begin{aligned}\varphi(X)&=a_{-m}X^{-m}+a_{-m+1}X^{-m+1}+\cdots+a_{-1}X^{-1}\\&+a_0+a_1X+a_2X^2+\cdots,a_i\in\mathbb{R},\end{aligned}$$

其中允许出现有限多个负指数①. 换言之，$\varphi(X)=X^{-m}f(X)$, 其中 $f(X)$ 是取自 $\mathbb{R}[[X]]$ 的通常的幂级数.

2. 设无限实数序列 $a_0,a_1,a_2,\cdots$ 从某项开始是周期的. 证明幂级数 $f(X)=a_0+a_1X+a_2X^2+\cdots$ 可以写成 $\mathbb{R}(X)$ 中的有理函数.

3. 证明形如 $f/p^n,n\geqslant1$, 的最简分式及其线性组合的集合是环 $P_0(X)$ 的一个子环 (见第 2 段最后的注记).

4. 令 $P=\mathbb{Z}_3$, 根据习题 3, 证明最简分式

$$\frac{a_1X+b_1}{X^2+1}+\frac{a_2X+b_2}{(X^2+1)^2}+\cdots\qquad a_i,b_i\in\mathbb{Z}_3$$

组成一个环 R, 带有无穷降链

$$R=R_1\supset R_2\supset\cdots\supset R_N\supset\cdots$$

其中子环 R_N 由分式 $(aX+b)/(X^2+1)^n$, $n\geqslant N$, 张成.

①这种情况下，称之为亚纯幂级数. ——译者注.

第 6 章　多项式的根

过去代数学研究的主要目的是求多项式的根. 这一领域在现代代数学中不再占据主导地位，但它的重要性仍然是毋庸置疑的. 事实上，许多数学问题最终都归结为计算某些具体多项式的根，或归结为对根的总体性质的描述. 我们在这一章中仅涉及根的最简单的性质，但这些性质已足够显示出复数域的特殊地位.

§1　根的一般性质

1. 根和线性因子　设 A 是一个有单位元的交换环，并且它包含在整环 R 中.

定义　元素 $c \in R$ 叫作多项式 $f \in A[X]$ 的 **根**(或 **零点**), 若 $f(c)=0$. 也称 c 是方程 $f(X)=0$ 的根.

我们必需考察真包含有 A 的环，理由很清楚，例如回忆多项式 $f(X)=X^2+1$ 在 $\mathbb{R}$ 中没有根，但在 $\mathbb{C}=\mathbb{R}[i]$ 中有根. 不过我们首先考察 $R=A$ 的情况.

定理 1(贝祖 (Bezout) 定理)　*元素 $c \in A$ 是多项式 $f \in A[X]$ 的根，当且仅当 $X-c$ 在环 $A[X]$ 中整除 f.*

证明　这个定理是我们以前证明过的一个一般论断的特例. 由带余除法 (第 5 章 §2 定理 5) 可见， $f(X)=(X-c)q(X)+r(X)$, 其中 $\deg\ r(X)<\deg(X-c)=1$. 于是 $r(X)$ 是常数. 用 c 代替 X(即运用第 5 章 §2 定理 2 的映射 Π_c), 得到 $f(c)=r$, 于是

$$f(X)=(X-c)q(X)+f(c) \tag{1}$$

特别地， $f(c)=0 \Leftrightarrow \quad f(X)=(X-c)q(X)$. □

用线性多项式 $X-c$ 去除一个系数在整环 A 中的多项式 $f(X)$ 用 **霍纳方法**(或

综合除法）比较方便，它比带余除法简单. 设

$$f(X)=a_0X^n+a_1X^{n-1}+\cdots+a_n,\quad a_i\in A.$$

根据公式 (1)

$$q(X)=b_0X^{n-1}+b_1X^{n-2}+\cdots+b_{n-1},\quad b_j\in A.$$

现在将 (1) 中的 $f(X)$ 和 $q(X)$ 换成上述表达式，比较 X 的相同方幂的系数 (从首项开始), 稍作调整得到

$b_0=a_0$	$\cdots$	$b_k=b_{k-1}c+a_k$	$\cdots$	$b_{n-1}=b_{n-2}c+a_{n-1}$	$f(c)=b_{n-1}c+a_n$

(2)

结果我们也算出了 f 在 $X=c$ 时的值，建立在综合除法上的递推公式 (2) 在实际计算中使用方便.

从定理 1 的观点来看，自然引出了下述更一般的

定义 元素 $c\in A$ 叫作多项式 $f\in A[X]$ 的 k **重根**(或 k **重零点**), 若 f 被 $(X-c)^k$ 整除，但不被 $(X-c)^{k+1}$ 整除. 1 重根叫作 **单根**(相应地 $k=2$ 和 $k=3$ 时分别叫作 **二重根** 和 **三重根**).

于是 $c\in A$ 是多项式 $f\in A[X]$ 的 k 重根，当且仅当 $f(X)=(X-c)^kg(X)$, 其中 $\text{g.c.d.}(X-c,g(X))=1$. 根据公式 (1), 后一条件亦可表示成不等式 $g(c)\neq 0$. 其次，注意到第 5 章 §2 定理 1,$\deg f=k+\deg g$, 从而 $k\leqslant \deg f$.

我们有下述重要的

定理 2 设 A是整环，$f\neq 0$ 是 $A[X]$ 中的多项式，$c_1,\cdots,c_r\in A$ 分别是 f 的 $k_1,\cdots,k_r$ 重根.

则

$$f(X)=(X-c)^{k_1}\cdots(X-c)^{k_r}g(X),$$
$$g(X)\in A[X],\quad g(c_i)\neq 0,\quad i=1,\cdots,r.$$

特别地，多项式 $f\in A[X]$ 的按照重数计算的根的个数不超过 f 的次数.

$$k_1+\cdots+k_r\leqslant \deg\ f. \tag{3}$$

证明 如果最开始给出的环 A 不是一个域,我们只要引入分式域 $Q(A)$, 并利用在环 $Q(A)[X]$ 中的唯一因子分解性即可 (在给定的情况下, 素因子是 $X-c_1,\cdots,X-c_r$, 见第 5 章 §3 和 §4 的结果). 但是没有必要用如此强有力的工具. 我们给出一个直接的证明.

对 r 作归纳，证明 f 可以被 $(X-c_1)^{k_1}\cdots(X-c_r)^{k_r}$ 整除，然后由 $\deg f=(k_1+\cdots+k_r)+\deg\ g$ 推出不等式 (3). 当 $r=1$ 时，结论是显然的. 设我们已经有

$$f(X)=(X-c_1)^{k_1}\cdots(X-c_{r-1})^{k_{r-1}}h(X).$$

因为 $c_r - c_1 \neq 0, \cdots, c_r - c_{r-1} \neq 0$, 并且 A 是整环, 故元素 c_r 不是多项式 $(X-c_1)^{k_1}\cdots(X-c_{r-1})^{k_{r-1}}$ 的根. 但 c_r 是多项式 f 的 k_r 重根, 即 $f(X) = (X-c_r)^{k_r}u(X)$. 所以 $h(c_r)=0$, 故 $h(X)=(X-c_r)^s v(X), s \leqslant k_r, v(c_r)\neq 0$. 我们有

$$(X-c_r)^{k_r}u(X) = f(X) = (X-c_1)^{k_1}\cdots(X-c_{r-1})^{k_{r-1}}(X-c_r)^s v(X).$$

利用整环 $A[X]$ 满足消去律断定 $s=k_r$. □

如果不假定 A 是整环, 定理 2 不再成立, 例如, 环 $\mathbb{Z}_8$ 上的多项式 $f(X)=X^3$: $f(0)=f(2)=f(4)=f(6)=0$,3 次多项式有 4 个根, f 在 $\mathbb{Z}_8[X]$ 上素因子的分解也是不唯一的: $f=X^3=X(X-4)^2=(X-2)(X^2+2X+4)=(X-6)(X^2-2X+4)$.

从定理 2 引出下述

推论 设 A 是一个整环, $f,g\in A[X]$ 是两个次数 $\leqslant n$ 的多项式, 如果它们在 A 中 $n+1$ 个不同的元素上取值相同, 则 $f=g$.

证明 令 $h=f-g$, 则 $\deg h \leqslant n$. 根据条件 $h(c_1)=\cdots=h(c_{n+1})=0$ 对两两不同的元素 $c_1,\cdots,c_{n+1}\in A$ 成立, 即次数 $\leqslant n$ 的多项式有不少于 $n+1$ 个根. 与不等式 (3) 的这一矛盾仅当 $h=0$ 时才能消除. □

2. 多项式函数 定理 2 的推论使我们有可能去解决前述 (见第 5 章 §2 第 1 段) 多项式的函数论观点与代数观点的联系问题. 每一个多项式 $f\in A[X]$ 对应于一个函数

$$\tilde{f}: A\to A,\quad a\mapsto f(a).$$

这些函数的集合构成一个环 A_{pol}, 叫作**多项式函数环**(或**整有理函数环**), 它是以点点相加和相乘为运算的函数环 $A^A=\{A\to A\}$ 的一个子环 (见第 4 章 §3 第 1 段例 3 和第 5 章 §2 定理 2). 用类似的方法还可以定义多变量的多项式函数.

我们已经在前面提到, 非零多项式 $X^2+X\in\mathbb{F}_2[X]$ 定义了一个零函数. 一般地, 如果 $f(X)=(X^p-X)g(X)$ 是 p 元有限域上的多项式, 则 $\tilde{f}$ 是一个零函数, 因为任取 $x\in\mathbb{F}_p, x^p-x=x(x^{p-1}-1)=0$. 仅当 $\deg f\leqslant p-1$ 时, 多项式 $f\in\mathbb{F}_p[X]$ 才由自己的函数 $\tilde{f}$ 确定. 任意多项式 $f\in\mathbb{F}_p[X]$ 可以用唯一确定的次数 $\leqslant p-1$ 的**约化**多项式 f^* 代替, 后者是用 X^p-X 去除 f 后得到的余式. 这时显然有 $\tilde{f}=\tilde{f}^*$.

在无限域或无限整环的情况下, 形式更为简单.

定理 3 *如果 A 是含有无限多个元素的整环, 则多项式环 $A[X]$ 到多项式函数环 A_{pol} 的映射 $f\mapsto\tilde{f}$ 是一个环同构.*

证明 事实上, 这是定理 2 推论的另一种表述. 我们只需要验证当多项式 $f\neq 0$ 时, $\tilde{f}\neq 0$, 即对某个 $a\in A, f(a)\neq 0$. 事实上若 $\deg f=n$, f 只有不超过 n 个零点. □

基于定理 3, 无限域 P 上的多项式环等同于多项式函数环 (将多项式函数记作 $f(x)$), 剩下的问题是, 如何根据 $\tilde{f}$ (实际上是根据多项式 f 的某些值) 重新构造多项式 f.

下面将给出所谓"插值"问题的精确描述. 设 $b_0, b_1\cdots, b_n$ 是域 P 的任意元素, 而 $c_0, c_1\cdots, c_n$ 是域 P 中两两不同的元素. 我们要找出一个次数 $\leqslant n$ 的多项式 $f\in P[X]$, 使得 $f(c_i)=b_i, i=0,1,\cdots,n$. 根据定理 2 的推论, 问题如果有解, 则解是唯一的. 但正如下述 **拉格朗日插值公式** 所指出的, 满足给定性质的多项式 f 永远存在:

$$f(X)=\sum_{i=0}^{n} b_i\frac{(X-c_0)\cdots(X-c_{i-1})(X-c_{i+1})\cdots(X-c_n)}{(c_i-c_0)\cdots(c_i-c_{i-1})(c_i-c_{i+1})\cdots(c_i-c_n)}. \tag{4}$$

事实上, 解的存在唯一性也可以从下述线性方程组得到:

$$a_0c_0^n+a_1c_0^{n-1}+\cdots+a_n=b_0$$

$$\cdots\cdots\cdots\cdots$$

$$a_0c_n^n+a_1c_n^{n-1}+\cdots+a_n=b_n$$

其中未知数 $a_0,\ a_1,\cdots,a_n$ 是所求多项式 f 的系数. 这个方程组的行列式是范德蒙行列式, 它不等于零, 故 a_i 可由克拉默公式求出. 但公式 (4) 更方便些, 它既简单又容易记忆. 有时 **牛顿插值公式**

$$f(X)=u_0+u_1(X-c_0)+\cdots+u_n(X-c_0)(X-c_1)\cdots(X-c_{n-1}) \tag{5}$$

有一些优越性, 其中系数 $u_0,u_1,\cdots,u_n$ 可以依次代入值 $X=c_0, X=c_1,\cdots,X=c_{n-1}$ 后确定. 插值公式 (4),(5) 在实际应用中用来计算以及函数 $\varphi:\mathbb{R}\to\mathbb{R}$ 的作图, 这个函数由表格给出或从实验得到. 如果人们不管用什么办法知道了函数 φ 在实直线 $\mathbb{R}$ 的一个区间 I 上"足够地好", 那么就力求用"光滑"函数, 比如多项式去近似地表示 φ(见图 24). 这时, 利用区间 I 内的点 $c_0,c_1,\cdots,c_n$ 和已知值 $\varphi(c_i)=b_i$ 作为插值点.

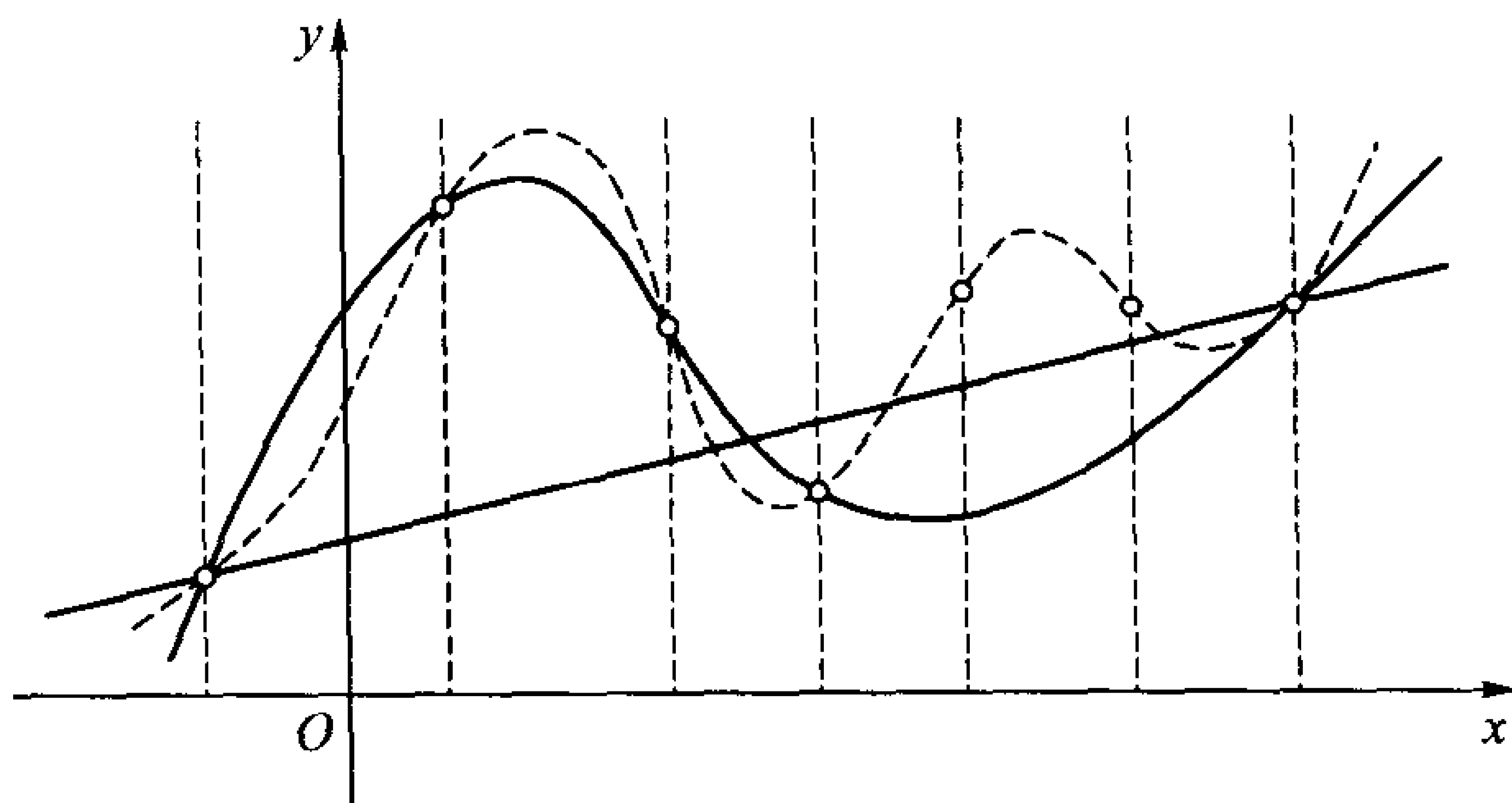


图 24

数学的某些领域就用于探讨插值点以及近似函数选取的精细问题. 应该指出, 插值法在超越数理论的发展中意义重大 (代数数和超越数的定义见第 5 章 §2), 所以, 插值问题引起了函数论, 数论和代数的综合兴趣.

最后我们指出，每一个既约分式 $f/g \in P(X)$ (见第 5 章 §4) 和每一个含有无限多个元素的扩域 $F \supset P$ 对应于一个分式函数 $\widetilde{f/g}$: $F_{(f/g)} \to F$, 它的定义域 $F_{(f/g)}$ 是从 F 中去掉有限个元素，即多项式 g 在 F 中的零点得到的. 可以证明，在所给的条件下，映射 $f/g \mapsto \widetilde{f/g}$ 是一一对应的. 我们不要求这一论证. 直观上它很清楚. 虽然有一一对应关系，但是在分式函数和既约分式之间存在着明显的区别. 分式函数 $x \mapsto 1/x$ 在点 $x = 0$ 处没有定义，可是既约分式 $\dfrac{1}{X}$ 的确定性问题一般不会出现.

3. 多项式环的微分法 如果把多项式看作函数，可以自然地给出下述定义. 设

$$f(X) = a_0X^n + a_1X^{n-1} + \cdots + a_{n-1}X + a_n$$

是域 P 上的 n 次多项式. 多项式

$$f'(X) = na_0X^{n-1} + (n-1)a_1X^{n-2} + \cdots + a_{n-1} \tag{6}$$

叫作 $f(X)$ 的 **导数**. 如果 $P = \mathbb{R}$ 是实数域，而 $\tilde{f}$ 是由 f 确定的多项式函数，则 (6) 式定义的导数与通常用下述极限

$$\lim_{\Delta x \to 0} \frac{\tilde{f}(x + \Delta x) - \tilde{f}(x)}{\Delta x}$$

定义的导数是一致的. 对任意域 P, 当多项式函数的连续性失去意义的情况下 (例如什么是 $\mathbb{Z}_p$ 中的收敛序列？), 需要根据形式定义 (6) 引出导数.

微积分中熟知的关系式仍然成立：

$$(\alpha f + \beta g)' = \alpha f' + \beta g', \quad \alpha, \beta \in P, \tag{7}$$

$$(fg)' = f'g + fg'. \tag{8}$$

(7) 式可以从 (6) 式以及多项式和的定义直接得到. 利用 (7) 式和多项式乘积的定义，对 (8) 式的检验可归结为 $f = X^k, g = X^l$ 的情况：

$$\begin{aligned}(X^{k+l})' &= (k+l)X^{k+l-1} = (k\,X^{k-1})X^l + X^k(l\,X^{l-1}) \\ &= (X^k)'X^l + X^k(X^l)'.\end{aligned}$$

作为 (8) 式的推广，对 k 作归纳易证下述公式

$$(f_1f_2\cdots f_k)' = \sum_{i=1}^{k} f_1\cdots f_{i-1}f_i'f_{i+1}\cdots f_k. \tag{9}$$

特别地

$$(f^k)' = kf^{k-1}f'.$$

现在我们试图将关系式 (7),(8) 用映射的术语 $\frac{d}{dX}$: $f \to f'$ 重新写过，($\frac{d}{dX}$ 叫作 **微分算子**). 先来考察任意环 R 上满足下述性质的映射 $D: R \to R$,

$$D(u+v) = Du + Dv, \tag{7'}$$

$$D(uv) = (Du)v + u(Dv). \tag{8'}$$

D 被称为 **导子**, 对研究环 R 非常有效，而它们的集合 $\mathrm{Der}(R)$ 成为一个有趣的数学对象，它是在一个宽广的数学领域 (李群和李代数) 中引入的.

(8′) 的推广是 **莱布尼茨公式**

$$D^m(uv) = \sum_{k=0}^{m} \binom{m}{k} D^k u\, D^{m-k} v, \tag{8''}$$

可以通过对 $m \geqslant 1$ 作归纳证明 (如果对 (8″) 应用 D, 利用 (8′) 和关系式 $\binom{m}{k-1} + \binom{m}{k} = \binom{m+1}{k}$ 就得到了 $m+1$ 时的公式 (8″)).

当 $R = P[X]$ 时，从关系式 (7′),(8′) 及法则

$$D(\lambda f) = \lambda Df, \qquad \lambda \in P,$$

直接推出

$$Df(X) = f'(X)DX.$$

于是多项式环 $P[X]$ 的任意导子由给定的多项式 DX 唯一确定. 当 $DX = 1$ 时，我们得到了一般的微分算子 $\frac{d}{dX}$.

4. 重因式 用 $f^{(m)}(X)$ 表示对 $f(X)$ 微分 m 次得到的结果. 显然,

$$f(X) = a_0X^n + a_1X^{n-1} + \cdots + a_n \Rightarrow f^{(n)}(X) = n!\, a_0, f^{(n+1)}(X) = 0.$$

如果 P 是一个特征零的域，则

$$\deg\ f' = \deg\ f - 1.$$

但是对于有限特征 p 的域，此事不真，因为

$$(X^{kp})' = kp\, X^{kp-1} = 0.$$

尽管如此，在一般情况下，通过考察多项式的导数，还是可以得到多项式的某些信息. 如果我们用 $(X-c)^2$ 去除任意多项式 $f \in P[X]$, 其中 $c \in F, F \supset P$ 是一个扩域，然后将 (线性) 余式写成 $(X-c)s + r$ 的形式，其中 $s, r \in F$, 我们得到

$$f = (X-c)^2 t + (X-c)s + r, \qquad f' = (X-c)[2t + (X-c)t'] + s.$$

以值 $X=c$ 代入此二式，得到 $r=f(c), s=f'(c)$, 于是

$$f(X)=(X-c)^2t(X)+(X-c)f'(c)+f(c).$$

这就证明了

定理 4 设 P 是任意域， F 是 P 的任意扩域. 多项式 $f\in P[X]$ 有重根 $c\in F$, 当且仅当 $f(c)=f'(c)=0$. □

例 1 在任意特征 p 的域中，若 n 不被 p 整除，则多项式 X^n-1 只有单根. 因为导数 nX^{n-1} 的根不可能是 X^n-1 的根.

下面假设 P 是特征为零的域，不失一般性， P 可以看作 $\mathbb{Q}$,$\mathbb{R}$ 或 $\mathbb{C}$ 之中的任意一个域. 设多项式 $f\in P[X]$,

$$f(X)=\lambda p_1(X)^{k_1}\cdots p_i(X)^{k_i}\cdots p_r(X)^{k_r}, \lambda\in P, \tag{10}$$

上述分解式中的首一既约多项式 $p_i(X)$ 叫作 f 的 k_i**重因式**(类似于 k 重根). 前面已经指出，得到分解式 (10) 在实践上是非常困难的. 我们将简述一种基于导数概念的方法，它可以判断出 $f(X)$ 在域 P(或其扩域) 上是否包含有重因式.

定理 5 设 $p(X)$ 是多项式 $f\in P[X]$ 的 k 重既约因式 ($k\geqslant 1$, $\deg\ p(X)\geqslant 1$). 则 $p(X)$ 是导数 $f'(X)$ 的 $(k-1)$ 重因式. 特别地，当 $k=1$ 时， f' 不被 $p(X)$ 整除.

证明 根据条件 $f(X)=p(X)^kg(X)$, 其中 $\text{g.c.d.}(p(X),g(X))=1$, 即 $g(X)$ 不能被 $p(X)$ 整除. 应用 (8) 和 (9) 式中的法则,

$$f'(X)=p(X)^{k-1}[kp'(X)g(X)+p(X)g'(X)].$$

只要证明方括号中的多项式不能被 $p(X)$ 整除即可. 否则， $p(X)$ 整除多项式 $kp'(X)g(X)$, 但这是不可能的 (见第 5 章 §3, 定理 3 和 4 的推论), 因为 $g(X)$ 不被 $p(X)$ 整除，而 $\deg\ k\,p'(X)<\deg\ p(X)$. □

注意，在定理 5 的证明过程中，实质上运用了 $p(X)$ 的既约性和 $\text{char}P=0$ 的条件.

推论 1 设多项式 $f(X)$ 的系数取自特征为零的域 P. 则下述两个条件等价:

i) f 在某个扩域 $F\supset P$ 中有 k 重根 c;

ii) $f^{(j)}(c)=0,\ 0\leqslant j\leqslant k-1$, 但 $f^{(k)}(c)\neq 0$.

证明 充分性：对线性因子 $p(X)=X-c$ 应用定理 5 k 次；必要性：取 P 的一个包含有 c 的扩域 F. □

推论 2 如果次数 $\geqslant 1$ 的多项式 $f\in P[X]$ 有分解式 (10), 则 f 及其导数 f' 的最大公因式有分解式

$$\text{g.c.d.}(f,f')=p_1(X)^{k_1-1}p_2(X)^{k_2-1}\cdots p_r(X)^{k_r-1} \tag{11}$$

(其中 g.c.d. 总是取首一多项式).

证明 根据定理 5, 多项式 $f(X)$ 的单因子 $p_i(X)$ 进入 $f'(X)$ 的分解式时指数为 k_{i-1},(见分解式 (10)), 即

$$f'(X) = p_1(X)^{k_1-1}p_2(X)^{k_2-1}\cdots p_r(X)^{k_r-1}.\ u(X),$$

其中 $\text{g.c.d.}(u,\ p_i) = 1,\ 1 \leqslant i \leqslant r$(约定 $p_i(X)^0 = 1$) . 所以根据整除性判别法 (见第 5 章 §3 第 2 段), $\text{g.c.d.}(f, f')$ 可用公式 (11) 计算. □

利用计算 $\text{g.c.d.}(f, f')$ 的公式 (11), 我们得到了一种方法, 可以去掉 $f(X)$ 分解式中的重因式. 考虑多项式

$$g(X) = \frac{f(X)}{\text{g.c.d.}(f, f')} = p_1(X)p_2(X)\cdots p_r(X),$$

$g(X)$ 包含有 $f(X)$ 的全部单因式, 但重数为 1. 重要的是, 多项式 $g(X)$ 可以通过欧几里得算法求出, 而不必实际知道 f 和 f' 的分解式.

例 2 多项式 $f(X) = X^5 - 3X^4 + 2X^3 + 2X^2 - 3X + 1$ 及其导数 $f'(X) = 5X^4 - 12X^3 + 6X^2 + 4X - 3$ 的最大公因式为首一多项式 $X^3 - 3X^2 + 3X - 1 = (X-1)^3$."无平方因式" 的多项式 $g(X) = f(X)/(X-1)^3 = X^2 - 1 = (X-1)(X+1)$ 有两个根: ± 1. 于是, $f(X) = (X-1)^4(X+1)$ 有 4 重根 $+1$ 和单根 -1.

5. 韦达公式 我们已经看到了一个良好的符号系统对线性方程组理论发展所起的作用, 特别是引出了行列式. 这是 18 世纪和 19 世纪初数学家们的功绩. 但是更早一些, 当代数还被当作 "解方程" 时, 由韦达和笛卡儿完善化的代数符号已经进入到多项式和代数方程的理论. 他们摆脱掩盖了一般规律的数字系数方程, 果断地转移到字母系数方程. 新的写法往往引出了新的结果. 笛卡儿完成了代数对几何的革命性的应用. 在本段中, 我们将给出他的前辈韦达的一些更朴素的成果.

设 n 次首一多项式 $f \in P[X]$ 在 P 中或 P 的某个扩域中有 n 个根 $c_1, c_2\cdots, c_n$, 容许有重根. 根据定理 2, 我们有分解式

$$f(X) = (X - c_1)(X - c_2)\cdots(X - c_n).$$

将 $f(X)$ 写成 X 方幂的一般形式:

$$f(X) = X^n + a_1X^{n-1} + \cdots + a_kX^{n-k} + \cdots + a_n,$$

将分解式中的所有一次二项式 $X - c_i$ 相乘, 合并同类项. 于是得到了系数 $a_1, \cdots, a_n$

通过根 $c_1, \cdots, c_n$ 的表达式:

$$
\begin{aligned}
a_1 &= -(c_1 + c_2 + \cdots + c_n), \\
&\cdots\cdots\cdots\cdots \\
a_k &= (-1)^k \sum_{i_1 < i_2 < \cdots < i_k} c_{i_1} c_{i_2} \cdots c_{i_k}, \\
&\cdots\cdots\cdots\cdots \\
a_n &= (-1)^n c_1 c_2 \cdots c_n.
\end{aligned} \tag{12}
$$

(12) 式称为 **韦达公式**.

如果多项式 f 不是首一的, 即首项系数 $a_0 \neq 1$, 则韦达公式给出了比值 a_i/a_0 的表达式, 与公式 (12) 类似.

韦达公式清楚地建立了任意多项式根与系数之间的关系, 它的美妙之处在于, 等式右边在根 $c_1, \cdots, c_n$ 的任何置换下都不改变. 这就给我们一个理由, 去引入 **对称函数** 的概念, 类似于行列式使我们引入了 **斜对称函数** 的概念.

根据第 1 章 §8 第 4 段的定义, 对称群 S_n 的元素 π 在 n 变元函数 $\tilde{f}(x_1, \cdots, x_n)$ 的作用由下述法则给出

$$(\widetilde{\pi \circ f})(x_1, \cdots, x_n) = \tilde{f}(x_{\pi(1)}, \cdots, x_{\pi(n)}).$$

函数 f 叫作 **对称的**, 若 $\widetilde{\pi \circ f} = \tilde{f}$ 对任意 $\pi \in S_n$ 成立. 如下定义的 **初等对称函数** $\mathbf{s}_k$ 是对称函数的一个例子:

$$\mathbf{s}_k(x_1, \cdots, x_n) = \sum_{1 \leqslant i_1 < i_2 < \cdots < i_k \leqslant n} x_{i_1} x_{i_2} \cdots x_{i_k} \tag{13}$$

利用初等对称函数可以将公式 (12) 改写成下述形式:

$$a_k = (-1)^k \mathbf{s}_k(c_1, \cdots, c_n), \quad k = 1, 2, \cdots, n \tag{12'}$$

所以精确到符号, 多项式 f 的系数 a_k 是函数 $\mathbf{s}_k$ 在多项式 f 的根集上的值. 注意到一个事实, 根据定义, $a_k \in P$, 但根 $c_1, \cdots, c_n$ 一般来说位于某个扩域 $F \supset P$ 中. 我们现在不涉及 F 的存在性问题. 但有时多项式到线性因式的分解是某些域 P 性质的直接推论.

例 3 考察有限域 $\mathbb{F}_p$ 上的多项式 $X^{p-1} - 1$(见第 4 章 §4 第 6 段). 我们知道对所有的 $x \in \mathbb{F}_p^*, X^{p-1} = 1$, 即所有的非零元素都是多项式 $X^{p-1} - 1$ 的根. 于是我们有分解式

$$X^{p-1} - 1 = (X-1)(X-2)\cdots(X-(p-1)) \tag{14}$$

在这里我们假设读者已经掌握了域 $\mathbb{F}_p$, 可以不困难地区分 $1, 2, \cdots, p-1$ 是作为通常 $\mathbb{Z}$ 中的整数, 还是域 $\mathbb{F}_p \cong \mathbb{Z}/p\mathbb{Z}$ 的元素 (代表剩余类 $\{i\}_p$). 根据 (12′) 和 (14), 当

$p>2$ 时，我们得到

$$\mathbf{s}_k(1,2,\cdots,p-1)\equiv 0(\mathrm{mod}p), k=1,\ 2,\ \cdots,\ p-2,$$
$$\mathbf{s}_{p-1}(1,2,\cdots,p-1)\equiv -1(\mathrm{mod}p).$$

后一个关系式的下述形式

$$(p-1)!+1\equiv 0(\mathrm{mod}p) \tag{15}$$

叫作 **威尔逊定理**, 这一公式是判定一个整数 p 是否为素数的充分必要条件. 事实上, 我们已经证明了 (15) 式对素数 p 成立. 另一方面，若 $p=p_1p_2 \Rightarrow (p-1)!=p_1t \Rightarrow (p-1)!+1\not\equiv 0(\mathrm{mod}p_1) \Rightarrow (p-1)!+1\not\equiv 0(\mathrm{mod}p)$.

习　　题

1. p 元域上的多项式函数环是整环吗？

2. 设 P 是无限域, f 是 $P[X_1,\cdots,X_n]$ 中的非零多项式. 基于定理 3 并对 n 作归纳证明, 存在 $a_1,\cdots,a_n\in P$, 使得 $f(a_1,\cdots,a_n)\neq 0$. 这就给出了 $P[X_1,\cdots,X_n]$ 与域 P 上 n 变元多项式函数环的同构.

3. 每个变元的次数皆小于 p 的非零多项式 $f\in\mathbb{Z}_p[X_1,\cdots,X_n]$ 具有习题 2 所述的性质：存在 $a_1,\cdots,a_n\in P$, 使 $f(a_1,\cdots,a_n)\neq 0$. 证明任意多项式 $f\in\mathbb{Z}_p[X_1,\cdots,X_n]$ 可表示为形式

$$f(X_1,\cdots,X_n)=\sum_{i=1}^{n} g_i(X_1,\cdots,X_n)(X_i^p-X_i)+f^*(X_1,\cdots,X_n),$$

其中 f^* 是一个 **约化** 多项式 ($\deg_{X_i} f^*\leqslant p-1, i=1,2,\cdots n$), 它的全次数 $\deg f^*\leqslant \deg f$. 由此断定, 从多项式环 $\mathbb{Z}_p[X_1,\cdots,X_n]$ 到 $\mathbb{Z}_p$ 上的 n 变元多项式函数环的映射 $f\mapsto\tilde{f}=\tilde{f}^*$ 是一个满射, 其核为 $L=\sum\limits_{i=1}^{n}(X_i^p-X_i)\mathbb{Z}_p[X_1,\cdots,X_n]$.

4. **定理**(谢瓦莱) 设 $f(X_1,\cdots,X_n)$ 是域 $\mathbb{Z}_p$ 上的 r 次齐次多项式 $(r<n)$. 证明方程 $f(X_1,\cdots,X_n)=0$ 至少有一个非平凡解.

提示： 因为 f 是齐次的, 显然有 $f(0,\cdots,0)=0$. 用反证法假设 $(a_1,\cdots,a_n)\neq 0 \Rightarrow f(a_1,\cdots,a_n)\neq 0$. 根据习题 3 和费马小定理, $g(X_1,\cdots,X_n)=1-f(X_1,\cdots,X_n)^{p-1}$ 的简约多项式为 $g^*(X_1,\cdots,X_n)=(1-X_1^{p-1})\cdots(1-X_n^{p-1})$. 但是

$$\deg g=(p-1)\deg f=(p-1)r<(p-1)n=\deg g*.$$

得到矛盾, 定理得证.

对论述稍加修改, 证明更一般的结论：方程 $f(X_1,\cdots,X_n)=0$ 的解的个数可以被 p 整除, (用两种方法计算和式 $\sum\limits_{x_1,\cdots,x_n\in\mathbb{Z}_p} g(X_1,\cdots,X_n)$).

5. 设 $f(x_1,\cdots,x_n)$ 是整系数二次型. 用同余的语言叙述谢瓦莱定理 (见习题 4), 可以断定当 $n\geqslant 3$ 时, 同余式

$$f(x_1,\cdots,x_n)\equiv 0(\mathrm{mod}p)$$

有非零解. 验证同余式 $x^2-2y^2\equiv 0(\mathrm{mod}5)$ 只有平凡解, 因而条件 $r<n$ 是本质的.

6. 若 f 是域 P 上的既约多项式，且 $\mathrm{char}P=0$, 证明 $\mathrm{g.c.d.}(f,f')=1$, 其中 f' 是 f 的导数.

7. 证明若 $f(X)$ 是特征为零的域上的多项式，则 $f'=0\Rightarrow f$ 是常数. 若 $f(X)$ 是特征 $p>0$ 的域上的多项式，则 $f'=0\Rightarrow f(X)=g(X^p)$ (其中 g 是另外的某个多项式).

8. 从第 3 段可知，多项式环 $P[X]$ 的每一个导子形如

$$T_u\colon f\mapsto uf',\quad u\in P[X].$$

证明下述论断：

i) 常数集 (从而在导子运算下取零值) 是 $P[X]$ 的子环;

ii) 两个导子的乘积 T_uT_v 一般来说不是导子，但如果 $\mathrm{char}P=p>0$, 则方幂 $(T_u)^p$ 是一个导子;

iii) **换位子**$[T_u,T_v]=T_uT_v-T_vT_u$ 是一个形如 T_w 的导子，其中 $w=uv'-u'v$.

9. 在 n 变元多项式环 $P[X_1,\cdots,X_n]$ 中可自然地引入对第 k 个变元的 **偏导子**

$$\frac{\partial}{\partial X_k}\colon X_1^{i_1}\cdots X_k^{i_k}\cdots X_n^{i_n}\mapsto i_kX_1^{i_1}\cdots X_k^{i_k-1}\cdots X_n^{i_n}.$$

i) 证明当 $\mathrm{char}P=0$ 时，关于 X_k 为常数，即在 $\dfrac{\partial}{\partial X_k}$ 下取零值的多项式的集合是 $n-1$ 个变元的多项式环 $P[X_1,\cdots,\hat{X}_k,\cdots,X_n]$.

ii) 设 $f(X_1,\cdots,X_n)$ 是一个 m 次齐次多项式，证明 **欧拉恒等式**

$$\sum_{k=1}^{n}X_k\frac{\partial f}{\partial X_k}=m\cdot f(X_1,\cdots,X_n).$$

反之，若 $\mathrm{char}P=0$, 则满足欧拉恒等式的多项式是 m 次齐次多项式，$m=1,2,3,\cdots$.

10. 证明多项式

$$X^n+a_1X^{n-1}+\cdots+a_n\in\mathbb{Z}_2[X]$$

没有线性因子，当且仅当

$$a_n(1+\Sigma a_i)\neq 0.$$

当 $n\leqslant 3$ 时，$\mathbb{Z}_2$ 上的全部既约多项式为：

$$X,X+1,X^2+X+1,\quad X^3+X+1,X^3+X^2+1.$$

写出 $\mathbb{Z}_2$ 上所有的 4 次和 5 次既约多项式 (其个数分别为 3 和 6).

11. 根据同余式

$$X^5-X-1\equiv(X^3+X^2+1)(X^2+X+1)(\mathrm{mod}2),$$

证明多项式 X^5-X-1 在 $\mathbb{Q}$ 上的既约性.

提示：利用高斯引理的推论 (第 5 章 §3) 和习题 10, 以及 $\mathbb{Z}_2[X]$ 的因子分解唯一性.

类似地，通过模 3 同余证明多项式 X^5-X-1 在 $\mathbb{Q}$ 上的不可分解性 (这样做更为简单).

§2 对称多项式

1. 对称多项式环 我们在上节的末尾定义了对称函数现在准备在整环 A 上的多项式环 $A[X_1,\cdots,X_n]$ 中定义类似的概念. §1 的定理 3 及其到多变元多项式和多变元函数的推广使我们可以将多项式环看作函数环的一个子环，似乎重新定义是多余的. 但注意到在该定理中要求 A 的元素是无限的，而我们希望给出一个一般性的结构.

$$(\pi\circ f)(X_1,\cdots,X_n)=f(X_{\pi(1)},\cdots,X_{\pi(n)}).$$

多项式 f 叫作 **对称的**, 若对所有的 $\pi\in S_n,\pi\circ f=f$. 和函数的情况一样，引入初等对称多项式 s_k:

$$\mathrm{s}_k(X_1,\cdots,X_n)=\sum_{1\leqslant i_1<i_2<\cdots<i_k\leqslant n}X_{i_1}X_{i_2}\cdots X_{i_k},\tag{1}$$

$$k=1,2,\cdots,n.$$

严格地说，考察系数在 $A[X_1,\cdots,X_n]$ 上以 Y 为新变量的多项式：

$$\begin{aligned}f(Y)&=(Y-X_1)(Y-X_2)\cdots(Y-X_n)\\&=Y^n-\mathrm{s}_1Y^{n-1}+\mathrm{s}_2Y^{n-2}+\cdots+(-1)^n\mathrm{s}_n,\end{aligned}\tag{2}$$

我们注意到， s_k 是对称多项式，恒等式 (2) 的左边在线性因子 $Y-X_1,\cdots,Y-X_n$ 的任意置换下不变.

注意到当我们在恒等式 (2) 的两端将 X_n 换成 0 时，得到

$$(Y-X_1)\cdots(Y-X_{n-1})X=Y^n-(\mathrm{s}_1)_0Y^{n-1}+\cdots+(-1)^{n-1}(\mathrm{s}_{n-1})_0Y,$$

其中 $(\mathrm{s}_k)_0$ 是在 s_k 中取 $X_n=0$ 得到的结果. 消去两端的 Y(将第 4 章 §3 的定理 1 应用于环 $A[X_1,\cdots,X_n,Y]$) 得到恒等式

$$\begin{aligned}&(Y-X_1)(Y-X_2)\cdots(Y-X_{n-1})\\&=Y^{n-1}-(\mathrm{s}_1)_0Y^{n-2}+\cdots+(-1)^{n-1}(\mathrm{s}_{n-1})_0.\end{aligned}\tag{3}$$

比较 (2) 和 (3), 我们断言 $(\mathrm{s}_1)_0,\cdots,(\mathrm{s}_{n-1})_0$ 是 $(n-1)$ 个变元 $X_1,\cdots,X_{n-1}$ 的初等对称多项式.

由于 $\tilde{\pi}:f\mapsto\pi\circ f$ 是多项式环 $A[X_1,\cdots,X_n]$ 的自同构，任意对称多项式及其乘积的线性组合仍然是对称多项式. 这就表明，全体对称多项式构成的环是$A[X_1,\cdots,X_n]$的子环. 我们的下一个目标是搞清楚这个子环的结构.

2. 对称多项式基本定理 下面指出得到对称多项式的一个最一般的方法. 任取多项式 $g\in A[Y_1,\cdots,Y_n]$, 并将 $Y_1,\cdots,Y_n$ 分别换成 $\mathrm{s}_1,\cdots,\mathrm{s}_n$. 所得多项式当然是对称多项式.

我们指出，在 g 中出现的单项式 $Y_1^{i_1}\cdots Y_n^{i_n}$ 用 $Y_k=\mathrm{s}_k(X_1,\cdots,X_n)$ 替换后成为 $X_1,\cdots,X_n$ 的齐次多项式，次数为 $i_1+2i_2+\cdots+ni_n$，因为 $\deg\mathrm{s}_k=k$. $i_1+2i_2+\cdots+ni_n$ 叫作单项式 $Y_1^{i_1}\cdots Y_n^{i_n}$ 的 **权**. 多项式 $g(Y_1,\cdots,Y_n)$ 的权 自然地定义为在 g 中出现的全部单项式的最大权.

关于对称多项式的基本论断是

定理 1 *设 $f\in A[X_1,\cdots,X_n]$ 是整环 A 上全次数为 m 的对称多项式. 则存在唯一的权为 m 的多项式 $g\in A[Y_1,\cdots,Y_n]$，使得*

$$f(X_1,\cdots,X_n)=g(\mathrm{s}_1,\cdots,\mathrm{s}_n).$$

并且多项式 g 的系数是 f 系数的整线性组合.

证明 我们曾经指出 (第 5 章，§2)，任意多项式 $f=f(X_1,\cdots,X_n)$ 可以写成不同次数的齐次型 f_m 的和：$f=f_0+f_1+\cdots+f_k$. 显然，这种写法是唯一的. 现在如果 f 是对称多项式，则型 f_m 也是对称的，因为 $\pi\circ f=\sum\pi\circ f_m$，而 $\tilde{\pi}:f_m\mapsto\pi\circ f_m$ 在 m 次型 f_m 上的作用是不变的. 于是，不失一般性，我们可以假定对称多项式 f 是齐次的. 下述论证分成若干部分.

1. 我们首先约定对 f 中的单项式进行字典排列 (按构造字典的原则排列)，即单项式 $u=aX_1^{i_1}X_2^{i_2}\cdots X_n^{i_n}$ 先于单项式 $v=bX_1^{j_1}X_2^{j_2}\cdots X_n^{j_n}$ (或大于单项式 $v:u>v$)，若序列 $i_1-j_1,i_2-j_2,\cdots,i_n-j_n$ 形如 $0,\cdots,0,t,\cdots$，其中 $t>0$. t 的右边可以出现负差 i_l-j_l. 按照字典序出现在第一个位置的单项叫作 f 的 **首项**，记作 FT(first term).

引理 1 *乘积 $h=h_1h_2\cdots h_r$ 中的首项是因子 $h_1,h_2,\cdots,h_r$ 的首项的乘积.*

事实上，当 $n=1$ 时，结论显然，如果

$$h=h(X_1,X_2,\cdots,X_n)=g_0(X_2,\cdots,X_n)X_1^s+g_1(X_2,\cdots,X_n)X_1^{s-1}+\cdots.$$

则 $\mathrm{FT}(h)=X_1^s\cdot\mathrm{FT}(g_0)$，现在取每个因子 h_i 按 X 方幂的展开式，并注意系数 $g_0(X_1,\cdots,X_n)$ 是怎样得到的，对 n 作归纳，得到所需的结论 $\mathrm{FT}(h)=\prod\limits_{i=1}^{r}\mathrm{FT}(h_i)$.□

2. 单项式 $v=aX_1^{i_1}X_2^{i_2}\cdots X_n^{i_n}$ 称为 **单调的**，若 $i_1\geqslant i_2\geqslant\cdots\geqslant i_n$.

引理 2 *对称多项式的最高次项永远是单调的.*

事实上，设 $\mathrm{FT}(f)=u=aX_1^{i_1}X_2^{i_2}\cdots X_n^{i_n}$. 假设对某个 $k\leqslant n-1$，有 $i_k<i_{k+1}$. 在 $u=aX_1^{i_1}\cdots X_k^{i_k}\cdot X_{k+1}^{i_{k+1}}\cdots X_n^{i_n}$ 中置换 X_k 和 X_{k+1}，得到单项式 $u'=aX_1^{i_1}\cdots X_k^{i_{k+1}}X_{k+1}^{i_k}\cdots X_n^{i_n}$ ，由于 f 是对称的，u' 在 f 中. 但显然 $u'>u$，因为 $X_1,\cdots,X_{k-1}$ 在 u 和 u' 中的指数相等，而 X_k 在 u' 中的指数大于 X_k 在 u 中的指数. 得到矛盾，引理得证. □

3. *多项式 $g(Y_1,\cdots,Y_n)$ 的存在性.* 设 $u=aX_1^{i_1}X_2^{i_2}\cdots X_n^{i_n}=\mathrm{FT}(f)$. 根据引理 2,$i_k\geqslant i_{k+1},1\leqslant k\leqslant n-1$. 因而我们可以考察对称多项式

$$f_{(1)}(X_1,\cdots,X_n)=f(X_1,\cdots,X_n)-a\mathrm{s}_1^{i_1-i_2}\mathrm{s}_2^{i_2-i_3}\cdots\mathrm{s}_n^{i_n},$$

对应的单项式 $aY_1^{i_1-i_2}Y_2^{i_2-i_3}\cdots Y_n^{i_n}$ 有权 $(i_1-i_2)+2(i_2-i_3)+\cdots+(n-1)(i_{n-1}-i_n)+ni_n=i_1+i_2+\cdots+i_n=\deg f$. 因为初等对称多项式 $\mathrm{s}_1,\mathrm{s}_2,\cdots,\mathrm{s}_n$ 的最高次项为 $X_1,X_1X_2,\cdots,X_1X_2\cdots X_n$, 故由引理 1，在 $a\mathrm{s}_1^{i_1-i_2}\mathrm{s}_2^{i_2-i_3}\cdots\mathrm{s}_n^{i_n}$ 中的最高次项是

$$\begin{aligned}&aX_1^{i_1-i_2}(X_1X_2)^{i_2-i_3}\cdots(X_1X_2\cdots X_{n-1})^{i_{n-1}-i_n}(X_1X_2\cdots X_n)^{i_n}\\=&aX_1^{i_1}X_2^{i_2}\cdots X_n^{i_n},\end{aligned}$$

即 $u=\mathrm{FT}(f)$. 于是 u 在 $f_{(1)}$ 中被消去，所以 $\mathrm{FT}(f)>\mathrm{FT}(f_{(1)})$. 还要指出，多项式 $f_{(1)}$ 的系数形如 $c-qa$, 其中 c,a 是多项式 f 的系数， $q\in\mathbb{Z}$.

设 $v=bX_1^{j_1}X_2^{j_2}\cdots X_n^{j_n}=\mathrm{FT}(f_{(1)})$, $b\in A$. 再次由引理 2 知 $j_1\geqslant j_2\geqslant\cdots\geqslant j_n$, 并根据前述论证，对称多项式

$$f_{(2)}(X_1,\cdots,X_n)=f_{(1)}(X_1,\cdots,X_n)-b\mathrm{s}_1^{j_1-j_2}\mathrm{s}_2^{j_2-j_3}\cdots\mathrm{s}_n^{j_n}$$

满足条件 $\mathrm{FT}(f_{(1)})>\mathrm{FT}(f_{(2)})$. 此外，多项式 $f_{(2)}$ 的系数形如 c_1-q_1b, 其中 $q_1\in\mathbb{Z}$, 而 c_1,b 是多项式 $f_{(1)}$ 的系数.

重复这一过程，我们得到一系列齐次对称多项式

$$f_{(k)}=f-a\mathrm{s}_1^{i_1-i_2}\cdots\mathrm{s}_n^{i_n}-b\mathrm{s}_1^{j_1-j_2}\cdots\mathrm{s}_n^{j_n}-\cdots$$

满足次数 $\deg f_{(k)}=\deg f$, 使得

$$\mathrm{FT}(f)>\mathrm{FT}(f_{(1)})>\mathrm{FT}(f_{(2)})>\cdots>\mathrm{FT}(f_{(k)})>\cdots\tag{4}$$

并且 $f_{(k)}$ 的系数是多项式 f 系数的 $\mathbb{Z}$ 线性组合. 因为给定次数的单项式只有有限个，(何况它们还是单调的), 不等式序列 (4) 必须中止，(即对于某个正整数 $k, f_{(k)}=0$); 我们得到了所需的结论 $f(X_1,\cdots,X_n)=g(\mathrm{s}_1,\cdots,\mathrm{s}_n)$, 其中 $g(Y_1,\cdots,Y_n)=aY_1^{i_1-i_2}Y_2^{i_2-i_3}\cdots Y_n^{i_n}+bY_1^{j_1-j_2}Y_2^{j_2-j_3}\cdots Y_n^{j_n}+\cdots$.

4. 唯一性 如果存在两个不同的表达式 $f=g_1(\mathrm{s}_1,\mathrm{s}_2,\cdots,\mathrm{s}_n)=g_2(\mathrm{s}_1,\mathrm{s}_2,\cdots,\mathrm{s}_n)$, 我们得到一个非零多项式 $g(Y_1,\cdots,Y_n)=g_1(Y_1,\cdots,Y_n)-g_2(Y_1,\cdots,Y_n)$, 权为 $\deg f$, 且 $g(\mathrm{s}_1,\cdots,\mathrm{s}_n)=0$, 如果 $aY_1^{k_1}Y_2^{k_2}\cdots Y_n^{k_n}$ 是 g 中的一个单项式，我们看到 $\mathrm{FT}(a\mathrm{s}_1^{k_1}\cdots\mathrm{s}_n^{k_n})=aX_1^{k_1}(X_1X_2)^{k_2}\cdots(X_1\cdots X_n)^{k_n}=aX_1^{k_1+k_2+\cdots+k_n}X_2^{k_2+\cdots+k_n}\cdots X_n^{k_n}$. 因此显然，不同的首项对应于 g 中不同的单项式. 它们当中有一个是最大的，即 $\mathrm{FT}(g(\mathrm{s}_1,\cdots,\mathrm{s}_n))\neq 0$, 与假设矛盾. □

关于唯一性的论断意味着 $\mathrm{s}_1,\cdots,\mathrm{s}_n$ 在 A 上是 **代数无关的**, 而环 $A[\mathrm{s}_1,\cdots,\mathrm{s}_n]$ 与 $A[X_1,\cdots,X_n]$ 同构 (尽管不言而喻， $A[\mathrm{s}_1(X_1,\cdots,X_n),\cdots,\mathrm{s}_n(X_1,\cdots,X_n)]$ 是 $A[X_1,\cdots,X_n]$ 中的真子集). 顺便指出当 $A=\mathbb{Z}$ 时，多项式 f 和 g 的系数是整数. 从定理 1 还导出一个有用的推论.

推论 设 $f(X) = X^n + a_1X^{n-1} + \cdots + a_{n-1}X + a_n$ 是域 P 上的单变元首一 n 次多项式，在某一扩域 $F \supset P$ 上有 n 个根 $c_1, \cdots, c_n$. 另一方面设 $h(X_1, \cdots, X_n)$ 是 $P[X_1, \cdots, X_n]$ 的任意对称多项式.

则用 c_i 替换 $X_i, i = 1, \cdots, n$, 所得的值 $h(c_1, \cdots, c_n)$ 在域 P 中.

证明 事实上，根据对称多项式基本定理，可以找到多项式 $g(Y_1, \cdots, Y_n) \in P[Y_1, \cdots, Y_n]$, 使得

$$h[X_1, \cdots, X_n] = g(\mathbf{s}_1(X_1, \cdots, X_n), \cdots, \mathbf{s}_n(X_1, \cdots, X_n)).$$

所以 $h(c_1, \cdots, c_n) = g(\mathbf{s}_1(c_1, \cdots, c_n), \cdots, \mathbf{s}_n(c_1, \cdots, c_n))$, 根据 §1 的韦达公式 (12), $\mathbf{s}_k(c_1, \cdots, c_n) = (-1)^k a_k \in P$，故 $g(-a_1, \cdots, (-1)^n a_n) \in P$. □

3. 待定系数法 对称多项式基本定理的证明有多种不同的方法，相应地，将给定的对称多项式用初等对称多项式表示出来也有多种不同的方法. 为了叙述一种最常用的方法，我们引入一类新的对称多项式. 为确定起见，我们将整环 A 取作环 $\mathbb{Z}$ 或域 $\mathbb{R}$. 设 $v = X_1^{i_1}X_2^{i_2}\cdots X_n^{i_n}$ 是一个单项式. 用 $S(v)$ 记从 v 经过变元的置换得到的所有不同的单项式的和. 例如

$$\mathbf{s}_k(X_1, \cdots, X_n) = S(X_1 \cdots X_k)$$

是第 k 个初等对称多项式.

$$\mathbf{p}_k(X_1, \cdots, X_n) = S(X_1^k) = X_1^k + X_2^k + \cdots + X_n^k, \quad k \geqslant 0, \tag{5}$$

叫作第 k 个 **幂和**. 显然，所有的 $S(v)$ 都是齐次对称多项式 (亦称为 **单演的**), 其全次数与 v 的次数相同. 因为 $S(v) = S(\sigma \circ v)$ 对任意 $\sigma \in S_n$ 成立，我们自然仅需对单调的单项式 v 考虑 $S(v)$. 显而易见， A 上的任意对称多项式 f 是系数取自 A 的 $S(v)$ 型多项式的线性组合：

$$f = \sum a_v S(v).$$

通常这样的表达方式一眼就可以看出来. 于是问题转化为找出 $S(v)$ 通过初等对称多项式的表达式.

每一个单调的单项式 $v = X_1^{i_1}X_2^{i_2}\cdots X_n^{i_n}$ 对应于一个对称多项式

$$g_v = g_v(X_1, \cdots, X_n) = \mathbf{s}_1^{i_1-i_2}\mathbf{s}_2^{i_2-i_3}\cdots\mathbf{s}_n^{i_n}, \tag{6}$$

它的首项就是 v. 按照定理 1 证明中的格式，我们详细给出通过初等对称多项式表达 $S(v)$ 的下述方法. 设 $\deg v = m$. 取整数 m 的一切单调划分

$$m = j_1 + j_2 + \cdots + j_n, \quad j_1 \geqslant j_2 \geqslant \cdots \geqslant j_n \geqslant 0,$$

使得 $w = X_1^{j_1}X_2^{j_2}\cdots X_n^{j_n} < v$. 考察所有的单项式 w 的集合 M_v. 任取 $w \in M_v$, 建立单项式 g_w(见 (6) 式). 我们已经知道

$$S(v) = g_v + \sum_{w \in M_v} n_w g_w, \tag{7}$$

此处 n_w 是某个整数. 在 (7) 式中用适当的整数, 通常是 0 和 1, 代入 $X_1, \cdots, X_n$, 可以依次求出待定的系数 n_w(这就是待定系数法名称的由来).g_v, g_w 和 $S_{(v)}$ 在这些整数下的值是已知的, 我们得到了关于 n_w 的一个相容的线性方程组.

例 1 $v = X_1^3, S(v) = \mathbf{p}_3(X_1, \cdots, X_n), \quad n \geqslant 3, g_v = \mathbf{s}_1^3,$

M_v	$X_1^2X_2$	$X_1X_2X_3$
g_w	$\mathbf{s}_1\mathbf{s}_2$	$\mathbf{s}_3$

这时, 方程 (7) 形如

$$\mathbf{p}_3 = \mathbf{s}_1^3 + a\mathbf{s}_1\mathbf{s}_2 + b\mathbf{s}_3.$$

如果 $X_1 = X_2 = 1$, 当 $i > 2$ 时 $X_i = 0$, 则 $\mathbf{p}_3 = 2, \mathbf{s}_1 = 2, \mathbf{s}_2 = 1, \mathbf{s}_3 = 0$.
如果 $X_1 = X_2 = X_3 = 1$, 当 $i > 3$ 时 $X_i = 0$, 则 $\mathbf{p}_3 = 3, \mathbf{s}_1 = 3, \mathbf{s}_2 = 3, \mathbf{s}_3 = 1$. 从方程组

$$2 = 2^3 + a \cdot 2 \cdot 1 + b \cdot 0,$$
$$3 = 3^3 + a \cdot 3 \cdot 3 + b \cdot 1$$

解得 $a = -3, b = 3$, 即 $\mathbf{p}_3 = \mathbf{s}_1^3 - 3\mathbf{s}_1\mathbf{s}_2 + 3\mathbf{s}_3$.

为了将幂和 $\mathbf{p}_k(X_1, \cdots, X_n)$ 表成 $\mathbf{s}_1, \mathbf{s}_2, \cdots, \mathbf{s}_n$ 的多项式, 我们有下述递推公式, 称之为 **牛顿公式**:

$$\mathbf{p}_k - \mathbf{p}_{k-1}\mathbf{s}_1 + \cdots + (-1)^{k-1}\mathbf{p}_1\mathbf{s}_{k-1} + (-1)^k k\mathbf{s}_k = 0, \tag{8}$$

若 $1 \leqslant k \leqslant n$;

$$\mathbf{p}_k - \mathbf{p}_{k-1}\mathbf{s}_1 + \cdots + (-1)^{n-1}\mathbf{p}_{k-n+1}\mathbf{s}_{n-1} + (-1)^n\mathbf{p}_{k-n}\mathbf{s}_n = 0, \tag{9}$$

若 $k > n$.

为了证明这些公式, 可在公式 (3) 中令 $Y = X_i$, 得到

$$X_i^n - \mathbf{s}_1X_i^{n-1} + \cdots + (-1)^{n-1}\mathbf{s}_{n-1}X_i + (-1)^n\mathbf{s}_n = 0.$$

用 X_i^{k-n} 乘以上式 $(k \geqslant n)$, 有

$$X_i^k - \mathbf{s}_1X_i^{k-1} + \cdots + (-1)^{n-1}\mathbf{s}_{n-1}X_i^{k-n+1} + (-1)^n\mathbf{s}_nX_i^{k-n} = 0,$$

然后对 i 从 1 到 n 求和, 我们就得到了公式 (9) 和 $k = n$ 时的公式 (8)($\mathbf{p}_0 = X_1^0 + \cdots + X_n^0 = n$). 进一步考察次数 $k \leqslant n$ 的齐次对称多项式 $f_{k,n}$(或 $k = -\infty$, 若 $f_{k,n} = 0$):

$$f_{k,n}(X_1, \cdots, X_n) = \mathbf{p}_k - \mathbf{p}_{k-1}\mathbf{s}_1 + \cdots + (-1)^{k-1}\mathbf{p}_1\mathbf{s}_{k-1} + (-1)^k k\mathbf{s}_k.$$

我们对 $r = n - k$ 作归纳, 证明 $f_{k,n}$ 恒等于 0. 当 $r = 0$ 时已证. 现在设 $X_n = 0$, 并注意到这时得到的对称多项式 $(\mathbf{s}_i)_0, (\mathbf{p}_i)_0$ 与定义在 $(n-1)$ 个变元 $X_1, \cdots, X_{n-1}$ 上

的多项式 $\mathbf{s}_i$ 和 $\mathbf{p}_i$ 重合 (见 (3) 和 (5)), 我们有等式

$$\begin{aligned}
&f_{k,n}(X_1,\cdots,X_{n-1},0)\\
&=(\mathbf{p}_k)_0-(\mathbf{p}_{k-1})_0(\mathbf{s}_1)_0+\cdots+(-1)^{k-1}(\mathbf{p}_1)_0(\mathbf{s}_{k-1})_0+(-1)^k k(\mathbf{s}_k)_0\\
&=f_{k,n-1}(X_1,\cdots,X_{n-1})=0,
\end{aligned}$$

因为 $n-1-k=r-1<r$, 故可用归纳假设.

关系式 $f_{k,n}(X_1,\cdots,X_{n-1},0)=0$ 表明, 多项式 $f_{k,n}$ 可以被 X_n 整除: $f_{k,n}=X_nf_1$. 利用 $f_{k,n}$ 的对称性, 这一多项式包含有因子 $X_1,X_2,\cdots,X_n$, 及它们的积 $\mathbf{s}_n=X_1X_2\cdots X_n$. 换言之,

$$f_{k,n}(X_1,\cdots,X_n)=\mathbf{s}_n(X_1,\cdots,X_n)\cdot h(X_1,\cdots,X_n). \tag{10}$$

分解式 (10) 仅当 $h=0$ 时才可能成立, 因为 $\deg\mathbf{s}_n=n$, 而 $\deg f_{k,n}=k<n$. 所以 $f_{k,n}=0$, 公式 (8) 得证. □

4. 多项式的判别式　考察环 $P[X_1,\cdots,X_n]$ 中的多项式

$$\Delta_n=\prod_{1\leqslant j<i\leqslant n}(X_i-X_j),$$

该式显然可表作范德蒙行列式

$$\Delta_n=\begin{vmatrix}1 & 1 & \cdots & 1\\ X_1 & X_2 & \cdots & X_n\\ \cdots & \cdots & \cdots & \cdots\\ X_1^{n-1} & X_2^{n-1} & \cdots & X_n^{n-1}\end{vmatrix}. \tag{11}$$

因为行列式是列的斜对称函数, 所以 $\pi\circ\Delta_n=\varepsilon\pi\Delta_n,\varepsilon_\pi$ 是置换 $\pi\in S_n$ 的符号. 于是 Δ_n^2 是对称函数, 根据对称多项式基本定理, 可表作初等对称函数的多项式

$$\Delta_n^2=\prod(X_i-X_j)^2=\mathrm{Dis}(\mathbf{s}_1,\cdots,\mathbf{s}_n).$$

以 $\mathbf{s}_1(X_1,\cdots,X_n),\cdots,\mathbf{s}_n(X_1,\cdots,X_n)$ 为变元的多项式 Dis 叫作 n 元组 $X_1,\cdots,X_n$ 的**判别式**. 其系数在 $\mathbb{Z}$ 中. 用元素 $x_i\in F$ 替换 $X_i,i=1,2,\cdots,n$(其中 F 是 P 的一个扩域), 我们就得到域 F 中任意 n 个元素组的判别式. 若元素 $X_1,\cdots,X_n$ 有相同者, 则该组的判别式为 0, 因为因子 X_i-X_j 中的某一个等于 0. 于是 Dis 能够区分 n 个元素两两不等和至少有两个相等的情况, 所以被称为判别式.

计算判别式的简便方法基于将 Δ^2 看作行列式 (11) 与其转置行列式的乘积: $\Delta_n^2=$

$\Delta_n \cdot {}^t\Delta_n$(回忆起对任意方阵 $A, \det{}^tA = \det A$). 事实上，由矩阵乘积的法则立即得到

$$\mathrm{Dis}(\mathbf{s}_1,\cdots,\mathbf{s}_n) = \begin{vmatrix} n & \mathbf{p}_1 & \mathbf{p}_2 & \cdots & \mathbf{p}_{n-1} \\ \mathbf{p}_1 & \mathbf{p}_2 & \mathbf{p}_3 & \cdots & \mathbf{p}_n \\ \mathbf{p}_2 & \mathbf{p}_3 & \mathbf{p}_4 & \cdots & \mathbf{p}_{n+1} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ \mathbf{p}_{n+1} & \mathbf{p}_{n+2} & \mathbf{p}_{n+3} & \cdots & \mathbf{p}_{2n-2} \end{vmatrix}, \tag{12}$$

其中 $\mathbf{p}_k$ 是我们已知的幂和 (5), 用递推公式 (8) 和 (9) 计算 $\mathbf{p}_k$, 我们就得到了 $\mathrm{Dis}(\mathbf{s}_1,\cdots,\mathbf{s}_n)$ 的显式. 特别地， $\mathbf{p}_1 = \mathbf{s}_1, \mathbf{p}_2 = \mathbf{s}_1^2 - 2\mathbf{s}_2$, 于是

$$\mathrm{Dis}(\mathbf{s}_1,\mathbf{s}_2) = \begin{vmatrix} 2 & \mathbf{s}_1 \\ \mathbf{s}_1 & \mathbf{s}_1^2 - 2\mathbf{s}_2 \end{vmatrix} = \mathbf{s}_1^2 - 4\mathbf{s}_2. \tag{13}$$

现在设首一多项式

$$f(X) = X^n + a_1X^{n-1} + \cdots + a_{n-1}X + a_n \in P[X],$$

在 P 或 P 的扩域 F 中有 n 个根 $c_1,\cdots,c_n$. 从韦达公式知，$a_k = (-1)^k\mathbf{s}_k(c_1,\cdots,c_n)$.

定义 由多项式 f 的根 $c_1,\cdots,c_n$ 组成的 n 元组的判别式，或等价地，判别式 $\mathrm{Dis}(\mathbf{s}_1,\cdots,\mathbf{s}_n)$ 当 $\mathbf{s}_k = (-1)^k a_k$ 时的值叫作多项式 f 的判别式，记作 $D(f)$. 亦称之为代数方程

$$f(X) = X^n + a_1X^{n-1} + \cdots + a_{n-1}X + a_n = 0 \tag{14}$$

的判别式.

显然 $D(f) \in P$(回忆定理 1 的推论).

从判别式的定义可知下述命题正确.

命题 $D(f) = 0$, 当且仅当方程 (14) 有重根 (即至少有一个根的重数 $k > 1$). □

回顾 §1 定理 5 的推论 2, 我们现在有两种方法不离开基础域就可以判断多项式 $f \in P[X]$ 有没有重根. 但判别式的意义远不止如此. 将公式 (13) 用于实系数二次三项式 $f(X) = X^2 + aX + b$, 得到 $D(f) = a^2 - 4b$, 这是在初等代数中熟知的公式. 特别地，$D(f)$ 的符号决定了方程 $x^2 + ax + b = 0$ 有两个实根还是一对共轭复根.

例 2 计算不完全三次方程

$$f(x) = x^3 + ax + b = 0 \tag{15}$$

的判别式. 在给定的情况下， $\mathbf{s}_4 = 0$, 根据递推公式计算 $\mathbf{p}_k$, 得到 $\mathbf{p}_1 = \mathbf{s}_1 = 0, \mathbf{p}_2 = \mathbf{s}_1^2 - 2\mathbf{s}_2 = -2a, \mathbf{p}_3 = \mathbf{s}_1^3 - 3\mathbf{s}_1\mathbf{s}_2 + 3\mathbf{s}_3 = -3b, \mathbf{p}_4 = \mathbf{s}_1^4 - 4\mathbf{s}_1^2\mathbf{s}_2 + 4\mathbf{s}_1\mathbf{s}_3 + 2\mathbf{s}_2^2 = 2a^2$. 从而公式 (12) 给出

$$D(f) = \begin{vmatrix} 3 & 0 & -2a \\ 0 & -2a & -3b \\ -2a & -3b & 2a^2 \end{vmatrix} = -4a^3 - 27b^2. \tag{16}$$

完全三次方程 $x^3+a_1x^2+a_2x+a_3=0$ 的判别式 $D(f)$ 表达起来更为复杂 (与 (16) 式相比), 但下述观察表明这种复杂性可以避免.

进行变量替换 $y=x+\dfrac{a_1}{n}$. 将 $x=y-\dfrac{a_1}{n}$ 代入方程 (14), 并利用二项式公式得到

$$g(y)=f\left(y-\frac{a_1}{n}\right)=y^n+ay^{n-2}+\cdots=0, \tag{17}$$

在新方程中, y^{n-1} 的系数为 0. 若知道了方程 (17) 的根 y_0, 我们很容易得到原始方程 (14) 的根 $x_0=y_0-\dfrac{a_1}{n}$. 因而不失一般性, 可设 $a_1=0$.

如果希望找到方程 (15) 解的一般公式 (这是中世纪数学家费罗、卡尔塔诺等人的巨大成就), 那么使用判别式 (16) 就是不可避免的 (见第 1 章 §2 公式 (2)).

5. 结式 在上一段命题中给出的 $D(f)$ 的基本性质, 亦可解释为多项式 f 和它的导数 f' 有公共根 (或公因子) 的判别法. 这一判别最终建立在欧几里得算法的基础之上. 这使我们有根据推测, 存在一个类似的法则, 用于直接从两个多项式 $f,g\in P[X]$ 的系数判断它们是否有公因子.

设

$$f(X)=a_0X^n+a_1X^{n-1}+\cdots+a_{n-1}X+a_n,$$

$$g(X)=b_0X^m+b_1X^{m-1}+\cdots+b_{m-1}X+b_m$$

是两个系数在域 P 中的多项式, 其中 $n>0,m>0$, 但不排除 $a_0=0$ 或 $b_0=0$ 的可能性.

定义 *多项式 f 和 g 的结式 $\mathrm{Res}(f,g)$ 是关于它们的系数的一个齐次多项式 (齐次多项式函数)(其中关于 $a_0,\cdots,a_n$ 为 m 次, 关于 $b_0,\cdots,b_m$ 为 n 次), 形如*

$$\mathrm{Res}(f,g)=\left|\begin{array}{cccccccc} a_0 & a_1 & \cdots & a_n & & & & \\ & a_0 & a_1 & \cdots & a_n & & & \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ & & & & a_0 & a_1 & \cdots & a_n \\ b_0 & b_1 & \cdots & b_m & & & & \\ & b_0 & b_1 & \cdots & b_m & & & \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ & & & b_0 & b_1 & & \cdots & b_m \end{array}\right| \begin{array}{l} \left.\begin{array}{l} \\ \\ \\ \\ \end{array}\right\} m\text{行} \\ \left.\begin{array}{l} \\ \\ \\ \\ \end{array}\right\} n\text{行} \end{array}$$

在结式的定义中, 包含关于多项式次数的断言. 它的证明可直接从行列式的性质得到: 若在前 m 行将 a_i 换成 ta_i, 则 $\mathrm{Res}(f,g)=t^m\mathrm{Res}(f,g)$, 然后利用第 5 章 §2 的习题 3.

现在来推导结式的基本性质.

R1 $\mathrm{Res}(f,g)=0$当且仅当 $a_0=0=b_0$ 或 f 和 g 在 $P[X]$ 中有次数 >0 的公因子.

证明 我们首先证明，条件 “$a_0=0=b_0$ 或 f 和 g 在 $P[X]$ 中有次数 >0 的公因子” 成立，当且仅当同时存在非零多项式 f_1,g_1, 使得

$$fg_1+f_1g=0,\quad \deg f_1<n,\quad \deg g_1<m. \tag{18}$$

事实上，设公因子 $h=\text{g.c.d.}(f,g)$ 使得 $\deg h>0$. 则 $f=hf_1, g=-hg_1$, 从而 $fg_1+gf_1=0$. 此外 $\deg f_1<n, \deg g_1<m$, (18) 式成立. 当 $a_0=0=b_0$ 时，我们亦可设 $f_1=f, g_1=-g$.

反之：设 (18) 式成立，若 $\text{g.c.d.}(f,g)=1$, 我们从 $P[X]$ 的因子分解唯一性 (见第 5 章 §3) 得到 $fg_1=-gf_1 \Rightarrow f|f_1, g|g_1$. 于是 $\deg f<n, \deg g<m$, 从而 $a_0=0=b_0$.

现在来证明条件 (18) 与 $\mathrm{Res}(f,g)=0$ 的等价性. 令

$$\begin{aligned}f_1&=c_0X^{n-1}+c_1X^{n-2}+\cdots+c_{n-1},\\ g_1&=d_0X^{m-1}+d_1X^{m-2}+\cdots+d_{m-1}.\end{aligned}$$

计算次数 $\leqslant n+m-1$ 的多项式 fg_1+gf_1 的系数，我们将条件 (18) 写成带有 $(n+m)$ 个未知量 $d_0,d_1,\cdots,d_{m-1},c_0,c_1,\cdots,c_{n-1}$ 和 $(n+m)$ 个方程的齐次线性方程组：

$$\begin{array}{lll}a_0d_0 & \cdots+b_0c_0 & \cdots=0,\\ a_1d_0+a_0d_1 & \cdots+b_1c_0+b_0c_1 & \cdots=0,\\ a_2d_0+a_1d_1+a_0d_2 & \cdots+b_2c_0+b_1c_1+b_0c_2 & =0,\\ \cdots\cdots & \cdots\cdots & \cdots\cdots\end{array} \tag{19}$$

方程组 (19) 的系数矩阵的行列式 (准确地说，系数矩阵转置的行列式) 恰为 $\mathrm{Res}(f,g)$. 于是，方程组 (19) 有非零解，当且仅当 $\mathrm{Res}(f,g)=0$, 而所有的非零解都给出一对满足条件 (18) 的多项式 f_1,g_1. □

R2 设多项式 f 和 g 均可在 $P[X]$ 中分解成线性因式：

$$\begin{aligned}f(X)&=a_0(X-\alpha_1)\cdots(X-\alpha_n),\\ g(X)&=b_0(X-\beta_1)\cdots(X-\beta_m).\end{aligned}$$

则

$$\mathrm{Res}(f,g)=a_0^m\prod_{i=1}^{n}g(\alpha_i)=(-1)^{mn}b_0^n\prod_{j=1}^{m}f(\beta_j)=a_0^mb_0^n\prod_{i,j}(\alpha_i-\beta_j).$$

证明 显然，如果这些公式成立，则应具有通用性，不依赖于多项式 f,g 的特殊形式. 我们不在这里深入探讨 “哲学” 原理，但它允许我们去考察 “一般情况”, 即设所有的 $g(\alpha_1),\cdots,g(\alpha_n)$ 和所有的 $f(\beta_1),\cdots,f(\beta_m)$ 是两两不同的.

因为 $\mathrm{Res}(g,f)=(-1)^{mn}\mathrm{Res}(f,g)$(见定义), 只要验证关系式 $\mathrm{Res}(f,g)=a_0^m\prod g(\alpha_i)$ 的正确性就足够了. 为此，引入一个新的变量 Y, 并在有理分式域 $P(Y)$ 上考察多项式 $f(X)$ 和 $g(X)-Y$. 将 b_m 换成 b_m-Y, 由结式的定义可得

$$\mathrm{Res}(f,g-Y)=(-1)^n a_0^m Y^n+\cdots+\mathrm{Res}(f,g)$$

是一个关于 Y 的 n 次多项式, 首项系数为 $(-1)^n a_0^m$, 常数项为 $\mathrm{Res}(f,g)$. 多项式 $f(X)$ 和 $g(X)-g(\alpha_i)$ 有公根 α_i, 故均可被 $X-\alpha_i$ 整除. 根据性质 R1 有 $\mathrm{Res}(f,g-g(\alpha_i))=0$.

根据贝祖定理，多项式 $\mathrm{Res}(f,g-Y)$ 可被 $g(\alpha_i)-Y$ 整除，$1\leqslant i\leqslant n$. 由于我们假定 $g(\alpha_i)$ 是两两不同的，故 $\mathrm{Res}(f,g-Y)=a_0^m\prod_{i=1}^n(g(\alpha_i)-Y)$. 令 $Y=0$, 即得所需等式. □

将第 4 段给出的判别式的定义推广到非首一多项式的情况，令

$$D(f)=a_0^{2n-2}\prod_{1\leqslant j<i\leqslant n}(\alpha_i-\alpha_j)^2=\left[a_0^{n-1}\prod_{j<i}(\alpha_i-\alpha_j)\right]^2,\quad a_0\neq 0.$$

R3　*下述公式成立:*

$$D(f)=(-1)^{\frac{n(n-1)}{2}}a_0^{-1}\mathrm{Res}(f,f'). \tag{20}$$

证明　根据 R2,

$$\mathrm{Res}(f,f')=a_0^{n-1}\prod_{i=1}^n f'(\alpha_i).$$

但

$$f'(\alpha_i)=a_0\prod_{j\neq i}(\alpha_i-\alpha_j),$$

这是在下述一般公式中令 $X=\alpha_i$ 得到的:

$$f'(X)=a_0\sum_{i=1}^n\prod_{j\neq i}(X-\alpha_j),$$

而 $f'(X)$ 可对乘积 $f(X)=a_0\prod_{j=1}^n(X-\alpha_j)$ 求导得到. 这样

$$\mathrm{Res}(f,f')=a_0^{2n-1}\prod_{i=1}^n\prod_{j\neq i}(\alpha_i-\alpha_j)=a_0(-1)^{\frac{n(n-1)}{2}}a_0^{2n-2}\prod_{j<i}(\alpha_i-\alpha_j)^2$$

$$=a_0(-1)^{\frac{n(n-1)}{2}}D(f).$$ □

习　题

1. 设 p 是奇数. 利用牛顿公式 (9) 和 (10) 证明

$$\sum_{i=1}^{p-1} i^m = \begin{cases} -1(\mathrm{mod} p) & 若m可被(p-1)整除, \\ 0 \ (\mathrm{mod} p) & 若m不被(p-1)整除. \end{cases}$$

2. 利用牛顿递推公式和克拉默公式证明下述 $\mathbf{p}_k$ 通过 $\mathbf{s}_k$ 以及 $\mathbf{s}_k$ 通过 $\mathbf{p}_k$ 的表达式:

$$\mathbf{p}_k = \begin{vmatrix} \mathbf{s}_1 & 1 & 0 & 0 & \cdots & 0 \\ 2\mathbf{s}_2 & \mathbf{s}_1 & 1 & 0 & \cdots & 0 \\ 3\mathbf{s}_3 & \mathbf{s}_2 & \mathbf{s}_1 & 1 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ (k-1)\mathbf{s}_{k-1} & \mathbf{s}_{k-2} & \mathbf{s}_{k-3} & \mathbf{s}_{k-4} & \cdots & 1 \\ k\mathbf{s}_k & \mathbf{s}_{k-1} & \mathbf{s}_{k-2} & \mathbf{s}_{k-3} & \cdots & \mathbf{s}_1 \end{vmatrix},$$

$$\mathbf{s}_k = \frac{1}{k!}\begin{vmatrix} \mathbf{p}_1 & 1 & 0 & 0 & \cdots & 0 \\ \mathbf{p}_2 & \mathbf{p}_1 & 1 & 0 & \cdots & 0 \\ \mathbf{p}_3 & \mathbf{p}_2 & \mathbf{p}_1 & 1 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ \mathbf{p}_{k-1} & \mathbf{p}_{k-2} & \mathbf{p}_{k-3} & \mathbf{p}_{k-4} & \cdots & 1 \\ \mathbf{p}_k & \mathbf{p}_{k-1} & \mathbf{p}_{k-2} & \mathbf{p}_{k-3} & \cdots & \mathbf{p}_1 \end{vmatrix}$$

3. 设 c_1, c_2, c_3 是多项式 X^3-X+1 的三个复根. 关于扩域 $\mathbb{Q}(c_1^{99}+c_2^{99}+c_3^{99})$ 可以说些什么?

4. 特征 $\neq 2$ 的域 P 上的多项式 $f(X_1,\cdots,X_n)$ 称为**斜对称的** (或**交错的**), 若 $\forall \pi \in S_n, (\pi \circ f)(X_1,\cdots,X_n) = \varepsilon_\pi f(X_1,\cdots,X_n)$(其中 ε_π 是置换 π 的符号). 于是 $\Delta_n = \prod_{j<i}(X_i - X_j)$ 是斜对称多项式的一个例子. 证明任意斜对称多项式 $f \in P[X_1,\cdots,X_n]$ 形如 $f = \Delta_n \cdot g$, 其中 g 是对称多项式.

提示: 将 f 看作系数取自 $P[X_1,\cdots,X_{n-1}]$ 中的 X_n 的多项式. 由于斜对称性, 当 $X_n = X_{n-1}$ 时, $f=0$, 所以 f 被 $X_n - X_{n-1}$ 整除.

5. 利用性质 R2 和多项式分裂域的存在性 (见下节) 证明

$$\mathrm{Res}(fg,h) = \mathrm{Res}(f,h)\cdot\mathrm{Res}(g,h).$$

6. 用习题 5 和 R3 推导公式

$$D(fg) = D(f)D(g)[\mathrm{Res}(f,g)]^2.$$

7. 结式 $\mathrm{Res}(f(X), X-a)$ 等于什么?

8. 证明 $D(X^n+a) = (-1)^{\frac{n(n-1)}{2}} n^n a^{n-1}$.

9. 设 $f(X) = X^{n-1}+X^{n-2}+\cdots+1$, 利用关系式 $X^n-1=(X-1)f(X)$ 和上题证明, $D(f) = (-1)^{\frac{(n-1)(n-2)}{2}}\cdot n^{n-2}$.

§3　域 $\mathbb{C}$ 的代数封闭性

1. 基本定理的叙述　设 P 是一个域，f 是 P 上的任意一个多项式. 正如在 §1 的第二段中指出的，f 确定的多项式函数 $\tilde{f}: P \to P$ 的性状，本质上依赖于域 P. 特别地，只要 $\deg f > 0$ 并对 P 采用下述定义，就有 $\mathrm{Im}\tilde{f} = P$.

定义　域 P 称为 **代数封闭的**, 如果环 $P[X]$ 中的每个多项式都可以分解成线性因式的乘积.

换言之, 域 P 是代数封闭的，如果只有一次多项式 (线性多项式) 在 P 上是既约的.

如果任一多项式 $f \in P[X]$ 在 P 上至少有一个根，那么，域 P 是代数封闭的. 事实上，这时有 $f(X) = (X-a)h(X), a \in P, h \in P[X]$, 但根据条件，多项式 h 在 P 中同样至少有一个根，即 $h(X) = (X-b)r(X), b \in P, r \in P[X]$. 继续这个过程，我们终止于把 f 完全分解为线性因式. 由于 f 是任意一个多项式，那么域 P 满足代数封闭性的定义.

尽管下述命题成立：对于任何一个域 P 都存在一个扩张 $\tilde{P} \supset P$, 使得 $\tilde{P}$ 是代数封闭的 (施坦尼茨定理), 但一开始就难于掌握的不仅是代数封闭扩张的结构，而且是此种扩张的含义本身. 特别令人高兴的是，我们事实上有一个显明的，非常重要的代数封闭域的例子，所谓 代数基本定理说的就是这个域.

定理 1　复数域 $\mathbb{C}$ 是代数封闭的.

现在我们用根的概念再次叙述这个基本定理.

任意一个次数 $n \geqslant 1$ 的复 (或实) 系数多项式 $f(X)$ 恰有 n 个按重数计算的复数根.

在求解代数方程还是代数学家中心工作的时代，定理 1 获得了 “基本定理” 这一极高的称誉. 今天，定理 1 已成为一系列重要命题之一.

基本定理的最早的严格证明是高斯于 1779 年给出的. 从那以后，出现了许多各种各样的，代数味道不同的证明. 在某种形式下用到域 $\mathbb{R}$ 和 $\mathbb{C}$ 的连续性质 (换言之，用到它们的拓扑); 甚至还有完全非代数的，基于复变量解析函数这一深刻概念的非常简洁的证明. 现在介绍一个立足于数学分析的初等知识, 发源于达朗贝尔、欧拉、高斯、柯西、阿尔冈等人的思想的证明. 最易懂的叙述是阿尔冈 (Argand R.,1814 年) 给出的，从那以后几乎所有的代数教科书中都采用这个证明.

2. 基本定理的证明　此证明的非代数部分，包含在两个辅助命题中，它们可以在任何一本分析教科书中找到.

1) 每个复多项式

$$f(z) = a_0 z^n + a_1 z^{n-1} + \cdots + a_{n-1} z + a_n, \quad n \geqslant 1, \tag{1}$$

是在平面 $\mathbb{C}$ 的任何一点都连续的函数. (函数 $f:\mathbb{C}\to\mathbb{C}$ 在点 $z_0\in\mathbb{C}$ 处连续，如果 $\lim\limits_{z\to z_0} f(z)=f(z_0)$; 换言之，对于任何邻域 $V(f(z_0))$ 都找得到一个邻域 $U(z_0)$ 使得对于每个 $z\in U(z_0)$ 有 $f(z)\in V(f(z_0))$.)

2) 每个在紧集 $K\subset\mathbb{R}^2$ 上的连续函数 $f:K\to\mathbb{R}$ 都在 K 上达到自己的最小值(紧集即闭的有界集合).

我们指出，其实应该说多项式函数 $\tilde{f}:\mathbb{C}\to\mathbb{C}$ 连续，不过我们使用在分析课本中通用的简洁说法. 我们用到的紧集将是某个半径 r 足够大的圆 $|z|\leqslant r$,r 的值以后再确定. 多项式 f 的自由项 $a_n=0$ 的平庸情形不予考虑，因为此时 f 有根 $z_0=0$.

为了从几何上弄清楚证明的思路，我们来想像 $\mathbb{R}^3$ 中对应于方程 $w=|f(z)|$ 的曲面： z 的值取在水平平面 $\mathbb{R}^2$ 上，而值 $|f(z)|$ 取在与 $\mathbb{R}^2$ 垂直的 w 轴的正方向上. $f(z)$ 在全平面 $\mathbb{C}$ 上的连续性蕴含着 $|f(z)|$ 的连续性. 需要证明的是，我们的曲面上至少有一个点 "落在" 水平平面 $\mathbb{R}^2$ 上 $(w=0)$. 我们把下面的论述分成几个步骤.

引理 1 存在正数 $r\in\mathbb{R}$, 使得 $|f(z)|>|f(0)|$ 对于一切满足 $|z|>r$ 的 $z\in\mathbb{C}$ 成立.

证明 对 $z\neq 0$ 有 $|f(z)|=|z|^n|a_0+g(z^{-1})|$, 其中 $g(u)=a_1u+a_2u^2+\cdots+a_nu^n\in\mathbb{C}[u]$. 从 g 在点 0 处的连续性推出，存在这样的实数 $\delta>0$, 使得 $|g(u)|\leqslant\dfrac{|a_0|}{2}$ 当 $|u|<\delta$ 时成立. 于是

$$|f(z)|\geqslant|z|^n(|a_0|-|g(z^{-1})|)\geqslant\frac{1}{2}|a_0||z|^n$$

当 $|z|>\delta^{-1}$ 时成立. 因此，剩下的问题是选取一个实数 $r>\delta^{-1}$ 使之满足不等式 $|a_0|r^n>2|a_n|$. □

推论 (关于最小值的柯西引理) 对于任意的多项式 $f\in\mathbb{C}[z]$, 存在 $z_0\in\mathbb{C}$ 使得 $|f(z_0)|=\inf\limits_{z\in\mathbb{C}}|f(z)|$.

事实上，根据命题 2), 连续函数 $|f(z)|$ 在圆 $D_r=\{z\in\mathbb{C}\,\big|\,|z|\leqslant r\}$ 内取到最小值，即存在 $z_0\in D_r$ 使 $|f(z_0)|=\inf\limits_{z\in D_r}|f(z)|$. 但由于 $|f(z_0)|\leqslant|f(0)|$, 而根据引理 1, 成立不等式 $|f(0)|\leqslant\inf\limits_{z\in\mathbb{C}\setminus D_r}|f(z)|$, 所以 $|f(z_0)|=\inf\limits_{z\in\mathbb{C}}|f(z)|$. □

引理 2 设 k 是任意一个整数, $k\geqslant 1$, 并设 $h\in\mathbb{C}[z]$ 是一个多项式且 $h(0)\neq 0$. 那么对于每个 $a\in\mathbb{C}^*$ 存在 $b\in\mathbb{C}$, 使得

$$|a+b^kh(b)|<|a|.$$

证明 从多项式 h 的连续性出发：存在 $\delta>0$ 使得当 $|z|<\delta$ 时 $|h(z)-h(0)|<\dfrac{|h(0)|}{2}$. 这使我们得到对于 $a+z^kh(z)=a+h(0)z^k+z^k(h(z)-h(0))$ 的估计式：

$$|a+z^kh(z)|\leqslant|a+h(0)z^k|+\frac{1}{2}|h(0)||z|^k \qquad (*)$$

在圆 $|z|<\delta$ 内成立.

现在选取复数 $b\in\mathbb{C}$ 使得

$$h(0)b^k=-ta,\quad 0<t<1$$

(下面我们将对实数 t 给予附加的限制). 根据第 5 章 §1 的定理 3, 只需取 b 为 $-tah(0)^{-1}\neq 0$ 的任意一个 k 次根即可. 我们得到 $|a+h(0)b^k|=(1-t)|a|$ 以及 $|h(0)|\frac{|b|^k}{2}=\frac{t|a|}{2}$, 将它们与 $(*)$ 联立, 当 $|b|<\delta$ 时就得到所需的不等式. 对于 $t=-h(0)a^{-1}b^k$ 施加限制 $t<|h(0)a^{-1}|\delta^k$ 就可以保证 $|b|<\delta$. 于是把值 $z=b,|b|<\delta$, 代入 $(*)$ 式, 我们终于得到

$$|a+b^kh(b)|\leqslant(1-t)|a|+\frac{1}{2}t|a|=\left(1-\frac{1}{2}t\right)|a|<|a|.$$ □

推论(达朗贝尔－阿尔冈引理)　*设 $f(z)$ 是 $\mathbb{C}$ 上的正次数多项式. 那么对应于每个使 $f(c)\neq 0$ 的点 $c\in\mathbb{C}$, 都有一个点 $c'\in\mathbb{C}$ 使*

$$|f(c')|<|f(c)|.$$

证明　多项式 $f(z+c)$ 与 $f(z)$ 一样不是常数, 将 $f(z+c)$ 按 z 的方幂展开:

$$f(z+c)=f(c)+b_kz^k+b_{k+1}z^{k+1}+\cdots+b_nz^n,\quad b_k\neq 0.$$

换言之,

$$f(z+c)=f(c)+z^kh(z),$$

其中

$$h(z)=b_k+b_{k+1}z+\cdots+b_nz^{n-k},\quad h(0)\neq 0.$$

在引理 2 的公式中代入值 $a=f(c)\neq 0$, 我们可以断定存在 $b\in\mathbb{C}$, 使得 $c'=b+c$ 时有不等式

$$|f(c')|=|f(b+c)|=|f(c)+b^kh(b)|<|f(c)|.$$ □

几何意义: 如果在曲面 $w=f(z)$ 上存在一个严格位于平面 $w=0$ 上方的点, 那么在曲面上必定存在另一点离平面 $w=0$ 更近.

基本定理 (定理 1) 证明的完成　根据引理 1 的推论, 存在这样的点 $z_0\in\mathbb{C}$, 使得对于一切 $z\in\mathbb{C}$ 有 $|f(z_0)|\leqslant|f(z)|$. 若 $f(z_0)\neq 0$, 则如引理 2 所断言的, 必存在 $z_0'\in\mathbb{C}$, 使得 $|f(z_0')|<|f(z_0)|$, 这是一个矛盾. □

暂且不对所述证明的缘由做任何解释, 我们给出一个与引理 1 明显类似的

引理 3(关于最高次项的模的引理)　*设 $f(z)$ 是形如 (1) 的具有任意的复系数 $a_0,a_1,\cdots,a_n,n\geqslant 1$, 的多项式. 令 $A=\max(|a_1|,\cdots,|a_n|),r=\frac{A}{|a_0|}+1$. 那么当 $|z|>r$ 时有不等式*

$$|a_0z^n|>|a_1z^{n-1}+\cdots+a_{n-1}z+a_n|.$$

证明 若取 $|z|>r$, 得到 $|a_0|>\dfrac{A}{|z|-1}$, 由此，根据复数模的运算法则 (见第 5 章 §1) 我们得到

$$\begin{aligned}|a_0z^n| &= |a_0||z|^n > \frac{A|z|^n}{|z|-1} > \frac{A(|z|^n-1)}{|z|-1}\\ &= A(|z|^{n-1}+\cdots+|z|+1) \geqslant |a_1||z|^{n-1}+\cdots+|a_{n-1}||z|+|a_n|\\ &= |a_1z^{n-1}|+\cdots+|a_{n-1}z|+|a_n| \geqslant |a_1z^{n-1}+\cdots+a_{n-1}z+a_n|.\end{aligned}$$ □

推论 1 设次数 $n\geqslant 1$ 的多项式 (1) 是实系数的. 那么对于一切绝对值足够大的 $x\in\mathbb{R}$(实数),$f(x)$ 的符号与最高次项 a_0x^n 的符号一致.

推论 2 实系数的奇次多项式必有实根.

证明 由于次数 n 是奇数，多项式映射 $\tilde{f}:\mathbb{R}\to\mathbb{R}$ 的最高次项 a_0x^n 对于正的和负的 $x\in\mathbb{R}$ 取相异的符号. 取绝对值足够大的 x, 根据推论 1 断定， $f(x)$ 将取相异的符号. 譬如说，若 $a_0>0$, 则 $f(-r)<0$ 而 $f(r)>0$, 其中 r 是引理 3 中所取的实数. 根据波尔查诺 - 柯西中值定理，在闭区间 $[-r,r]$ 上连续而在其两端取相异符号的连续函数 f, 必在区间的某点处取零值: $\exists c\in[-r,r]$, 使 $f(c)=0$(事实上， $f(x)$ 取遍介于 $f(-r)$ 和 $f(r)$ 之间的一切值). 同样的论述也适用于 $a_0<0$. □

3. 基本定理的又一个证明 在第 2 段中引入的定理 1 的基于几何直观证明，不仅给热爱代数的读者留下了不满足的感觉，也给 20 世纪的数学家们不满足的感觉. 难怪高斯一遍遍地思考基本定理，并整整给出了四个证明. 企图最少地用数学分析，而最大限度地用代数方法来进行论证. 这种 “代数的” 证明发端于欧拉、拉格朗日、高斯和拉普拉斯，后来获得了与伽罗瓦的一般理论相一致的典范形式. 我们一点都不涉及伽罗瓦理论，只希望感受我们熟知的技巧的风格. 整个证明分成两部分.

1) 对于任何次数 $n\geqslant 1$ 的多项式 $f\in P[z]$ 都存在一个**分裂域**, 即域 P 的一个最小扩张 F, 在 F 中含有多项式 f 的全部根. 记作 $F=P(u_1,\cdots,u_n)$ 以及 $f(z)=a_0(z-u_1)(z-u_2)\cdots(z-u_n)$.

为方便起见，我们还认为 f 是首一的 $(a_0=1)$. 对于每个多项式 $f\in P[z]$, 分裂域 $F\supset P$ 的存在性及精确到同构的唯一性，乃是泛代数结构的一个推论，我们将在 [BAⅢ] 中谈到泛代数结构. 回忆在第 4 章 §3 第 2 段中剩余类环 $\mathbb{Z}_m$ 的构造，这种泛代数的结构与基本域 P 的特性无关，唯一性一般并不需要. 作为一个例子，我们指出 $\mathbb{R}$ 上的多项式 z^2+1 的分裂域是复数域 $\mathbb{C}$.

2) 如果为了不使叙述变得困难，我们承认第 1) 部分，那么第 2) 部分就成为我们熟知的一般原理 (数学归纳法原理及过渡到对称函数的原理) 的一个极好的应用实例，我们来给出全部细节.

根据代数封闭域定义后面的注记，必须确定多项式 (1) 至少存在一个复根. 首

先假定它的系数都是实数，同时不失一般性假定 $a_0 = 1, a_n \neq 0$. 设

$$\deg f = 2^m n_0,$$

其中 n_0 是奇整数. 如果 $m = 0$, 那么根据引理 2, 多项式 f 有实根. 对 m 实施归纳法，我们认为定理对于一切次数为 $2^{m'} n_0'$, $m' \leqslant m - 1$ 的实系数多项式成立 (对于奇数因子 n_0' 不加任何限制). 我们指出，根据引理 3 的推论 2, 对应于值 $m = 0$ 的归纳法出发点已成立 (唯一的一处非代数性质).

我们来考察多项式 $(z^2+1)f(z)$ 的分裂域 F, 根据 1) 这个域存在且包含 $\mathbb{C}$ 作为其子域. 设 $u_1, \cdots, u_n$ 是多项式 f 在 F 中的根. 我们考察 F 中的元素

$$v_{ij} = u_i u_j + a(u_i + u_j), \qquad 1 \leqslant i < j \leqslant n, \tag{2}$$

其中 a 是某个固定的实数. 或许应该写成 $v_{ij}(a)$, 但我们不这样写，为的是不使记号太复杂. 形如 (2) 的元素的个数 n' 等于

$$n' = \begin{pmatrix} n \\ 2 \end{pmatrix} = \frac{n(n-1)}{2} = \frac{2^m n_0(2^m n_0 - 1)}{2} = 2^{m-1} n_0', \tag{3}$$

其中 n_0' 是奇整数.

环 $F[z]$ 中的多项式

$$f_a(z) = \prod_{1 \leqslant i < j \leqslant n} (z - v_{ij}) = z^{n'} + b_1 z^{n'-1} + \cdots + b_{n'}$$

的次数是 n', 而根据定义，(2) 中的全体元素恰是它的全部根. 根据 §1 中的韦达公式 (12), 多项式 $f_a(z)$ 的系数 $b_1, \cdots, b_{n'}$, 精确到符号是 v_{ij} 的初等对称函数 $\mathbf{s}_k$. 在 $\mathbf{s}_k(v_{12}, v_{13}, \cdots, v_{n-1,n})$ 中代入元素 v_{ij} 用 $u_1, \cdots, u_n$ 表出的式子，我们就得到函数

$$h_k(u_1, \cdots, u_n) = \mathbf{s}_k(\cdots, u_i u_j + a(u_i + u_j), \cdots), \quad k = 1, \cdots, n',$$

它仍是对称的. 其实，对于任何置换 $\pi \in S_n$(S_n 是 n 阶对称群) 我们令

$$\hat{\pi} \circ v_{ij} = u_{\pi(i)} u_{\pi(j)} + a\big(u_{\pi(i)} + u_{\pi(j)}\big) = v_{\pi(i),\pi(j)}$$

(或者 $v_{\pi(j),\pi(i)}$, 如果 $\pi(i) > \pi(j)$ 的话), 因此置换 π 诱导出元素 (2) 的集合上的一个置换 $\hat{\pi}$. 根据对称性，$\mathbf{s}_k(v_{12}, v_{13}, \cdots, v_{n-1,n})$ 在自变量的置换之下不变，因此

$$\begin{aligned}(\pi \circ h_k)(u_1, \cdots, u_n) &= \mathbf{s}_k(\hat{\pi} \circ v_{12}, \hat{\pi} \circ v_{13}, \cdots, \hat{\pi} \circ v_{n-1,n}) \\ &= \mathbf{s}_k(v_{12}, v_{13}, \cdots, v_{n-1,n}) = h_k(u_1, \cdots, u_n).\end{aligned}$$

我们指出，$h_k(u_1, \cdots, u_n)$ 是仅与 $a \in \mathbb{R}$ 有关的实系数对称多项式 $h_k(X_1, \cdots, X_n)$ 当 $X_i = u_i, i = 1, \cdots, n$, 时的值.

根据对称多项式基本定理 (§2 的定理 1), 存在实系数多项式 $g_k(Y_1,\cdots,Y_n)$ 使得 $h_k(X_1,\cdots,X_n)=g_k(\mathbf{s}_1(X_1,\cdots,X_n),\cdots,\mathbf{s}_n(X_1,\cdots,X_n))$. 可见

$$\begin{aligned}(-1)^k b_k = h_k(u_1,\cdots,u_n) &= g_k(\mathbf{s}_1(u_1,\cdots,u_n),\cdots,\mathbf{s}_n(u_1,\cdots,u_n))\\ &= g_k(-a_1,\cdots,(-1)^n a_n)\in\mathbb{R}\end{aligned}$$

(其中, a_i 是首一多项式 $f\in\mathbb{R}[z]$ 的系数).

于是, 对于任意 $a\in\mathbb{R}$, 多项式 $f_a(z)$ 的系数 b_k 都是实数. 因为 $\deg f_a=n'=2^{m-1}n_0'$(见 (3) 式) 根据归纳假设, f_a 必有一个复根, 此根当然应与数 v_{ij} 中的一个重合. 改变我们的参数 $a\in\mathbb{R}$, 得到另外的实系数多项式 $f_a(z)$. 对应于这些多项式中的每一个, 都有一对指标 $i<j$(依赖于 a), 使得元素 $v_{ij}=u_iu_j+a(u_i+u_j)\in F$ 含在域 F 的子域 $\mathbb{C}$ 中. 由于共有 $\begin{pmatrix} n\\ 2\end{pmatrix}$ 个不同的指标对 $i<j$, 而实数 $a\in\mathbb{R}$ 有无穷多个, 所以存在两个不同的实数 a,a', 确定了同一对指标, $i=1,j=2$(这只是根 $u_1,\cdots,u_n$ 的编号问题), 对于这对指标

$$\begin{aligned}&u_1u_2+a(u_1+u_2)=c,\\ &u_1u_2+a'(u_1+u_2)=c' \qquad (a\neq a')\end{aligned}$$

是复数. 从这个方程组推出

$$u_1+u_2=\frac{c-c'}{a-a'},\qquad u_1u_2=c-a\frac{c-c'}{a-a'}$$

属于域 $\mathbb{C}$. 这时, 元素 u_1,u_2 是复系数二次多项式

$$(z-u_1)(z-u_2)=z^2-(u_1+u_2)z+u_1u_2$$

的根. 根据已知的公式

$$u_1,u_2=\frac{u_1+u_2}{2}\pm\sqrt{\left(\frac{u_1+u_2}{2}\right)^2-u_1u_2}\ ,$$

u_1,u_2 也是复数. 于是, 对于所考察的实系数多项式 $f(z)$ 我们找到了甚至两个复根.

现设 $f(z)$ 是具有任意的复系数的形如 (1) 的多项式 (可以认为 $a_0=1$, 但这并不重要). 把全体 a_i 都改变成它们的复共轭数, 我们就得到多项式

$$\bar{f}(z)=\bar{a}_0z^n+\bar{a}_1z^{n-1}+\cdots+\bar{a}_{n-1}z+\bar{a}_n.$$

引入多项式

$$e(z)=f(z)\bar{f}(z)=e_0z^{2n}+e_1z^{2n-1}+\cdots+e_{2n},$$

它的次数是 $2n$, 具有系数

$$e_k = \sum_{i+j=k} a_i \bar{a}_j, \qquad k = 0, 1, \cdots, 2n.$$

由于共轭运算 $z \to \bar{z}$ 是域 $\mathbb{C}$ 的 2 阶自同构 (第 5 章 §1 定理 1), 所以 $\bar{e}_k = \sum\limits_{i+j=k} \bar{a}_i a_j = e_k$, 这就表明 $e_k \in \mathbb{R}$. 根据已证明的事实，实系数多项式 $e(z)$ 至少有一个复根 c:

$$f(c)\bar{f}(c) = e(c) = 0.$$

由此推出，要么 $f(c) = 0$ 从而定理获证，要么 $\bar{f}(c) = 0$, 即 $\bar{a}_0 c^n + \bar{a}_1 c^{n-1} + \cdots + \bar{a}_{n-1} c + \bar{a}_n = 0$. 对等式两边取复共轭，我们得到 $a_0 \bar{c}^n + a_1 \bar{c}^{n-1} + \cdots + a_{n-1}\bar{c} + a_n = 0$, 即 $f(\bar{c}) = 0$. □

域 $\mathbb{C}$ 的代数封闭性 (同样地，多项式存在分裂域的事实) 适宜于用来解决各种问题.

例 设 $S_0(f)$ 是多项式 $f \in \mathbb{C}[X]$ 的一切不同的根的集合，而 $S_1(f)$ 是它的一切 "单位" 的集合： $d \in S_1(f) \Longleftrightarrow f(d) = 1$. 现设 f, g 是 $\mathbb{C}[X]$ 中的两个多项式. 求证

$$S_0(f) = S_0(g), \quad S_1(f) = S_1(g) \Longrightarrow f(X) = g(X).$$

由于显然有 $S_0(f) \bigcap S_1(f) = \varnothing$, 所以根据 §1 的结果只需证明 $|S_0(f) \bigcup S_1(f)| \geqslant n+1$, 其中 $n = \deg f$. 根据定理 1

$$f(X) = a_0 \prod_{i=1}^{\nu} (X - c_i)^{s_i}, \quad f(X) - 1 = a_0 \prod_{j=1}^{\mu} (X - d_j)^{t_j}, \ c_i, d_j \in \mathbb{C}$$

其中

$$\sum s_i = n = \sum t_j, \quad \nu + \mu = |S_0(f) \bigcup S_1(f)|.$$

根据 §1 定理 5, 我们有

$$f(X)' = (f(X) - 1)' = \prod_{i=1}^{\nu} (X - c_i)^{s_i - 1} \prod_{j=1}^{\mu} (X - d_j)^{t_j - 1} \cdot h(X),$$

因此 $(n - \nu) + (n - \mu) \leqslant \deg f(X)' = n - 1$. 从而

$$\nu + \mu \geqslant n + 1.$$

代数基本定理的新证明不时地出现，成为先进数学思想的应用实例. 我们注意一下拓扑的证明，其中用到同伦、映射的阶、曲线的阶、临界点等概念. 可从下述初等入门教科书中了解这些概念:

1. Стинрод Н., Чинн У. Первые понятия топологии. — М.: Мир, 1967. (《拓扑学的基本概念》)

2. Милнор Дж., Уоллес А. Дифференциальная топология. — М.: Мир, 1972. (《微分拓扑学》)

3. Торп Дж. Начальные главы дфференцальной геометрии. — М.: Мир, 1982. (《微分几何入门》)

§4 实系数多项式

1. $\mathbb{R}[X]$中的因式分解 从 §3 的定理 1 推出，$\mathbb{C}[X]$ 中的每个 n 次多项式可以唯一地 (精确到因子的次序) 写成如下形式:

$$f(X) = a(X - c_1)(X - c_2) \cdots (X - c_n),$$

其中 $a \neq 0, c_1, \cdots, c_n$ 是复数. 现设 $f(X) = X^n + a_1X^{n-1} + \cdots + a_{n-1}X + a_n$ 是具有实系数 $a_1, \cdots, a_n$ 的首一多项式，并设 c 是它的一个复根：$c = u + iv, v \neq 0$. 对于关系式 $f(c) = 0$ 施行复共轭自同构，如同在 §3 定理 1 的第 2 个证明中所做的那样，我们就得到 $f(\bar{c}) = 0$, 因为 $\bar{a}_i = a_i$. 于是，$f(X)$ 被二次多项式

$$g(X) = (X - c)(X - \bar{c}) = X^2 - (c + \bar{c})X + c\bar{c} = X^2 - 2uX + (u^2 + v^2)$$

整除，$g(X)$ 的判别式是负的，$D(g) = 4u^2 - 4(u^2 + v^2) = -4v^2 < 0$. 条件 $D(g) < 0$ 等价于二次多项式 $g \in \mathbb{R}[X]$ 在 $\mathbb{R}$ 上是既约的.

其次设 k 是多项式 $f(X)$ 的根 c 的重数，而 $l \leqslant k$ 是根 $\bar{c}$ 的重数，那么 $f(X)$ 被多项式 g(X) 的 l 次幂整除：

$$f(X) = g(X)^l q(X).$$

$\mathbb{R}[X]$ 中的两个多项式的商 $q(X)$ 还是 $\mathbb{R}[X]$ 中的多项式，并且当 $k > l$ 时，元素 $c \in \mathbb{C}$ 是它的 $k - l$ 重根，同时 $\bar{c}$ 却不是根. 但是我们已经看到这是不可能的. 这表明 $k = l$($l \geqslant k$ 时可作类似处理), 于是，$\mathbb{R}[X]$ 中的任何多项式的复根都是两两共轭的，对于唯一因子分解整环 $\mathbb{R}[X]$ 的元素下述论断成立.

定理 1 任何一个首一 n 次多项式 $f \in \mathbb{R}[X]$ 都唯一地(精确到因子的次序) 分解成 $m \leqslant n$ 个对应于实根 $c_1, \cdots, c_m$ 的线性因式 $X - c_i$ 以及 $\dfrac{n-m}{2}$ 个对应于复共轭根对的二次既约因式的乘积.

注记 1) $\mathbb{R}[X]$ 中的既约多项式要么是线性的，要么是具有负判别式的二次多项式.

2) 用定理 1 的符号，我们有

$$D(f) = (-1)^{\frac{n-m}{2}} |D(f)|,$$

也就是说，判别式的符号由复共轭根对的数目决定．这个等式可以直接从判别式的定义得到，也可以从 §2 练习 6 的公式得到．

例 1　$g(X)=X^{2n}+1$．由于 $g(X)$ 没有实根，而其复根 $c_k=\cos\dfrac{2k-1}{2n}\pi+i\sin\dfrac{2k-1}{2n}\pi, 1\leqslant k\leqslant 2n$(按第 5 章 §1 中的公式 (16) 确定)，都是单根，所以 $g(X)$ 的实既约因子的指数都是 1．显然 $\bar{c}_k=c_{2n+1-k}, k=1,\cdots,n$，从而 $(X-c_k)(X-\bar{c}_k)=X^2-\left(2\cos\dfrac{2k-1}{2n}\pi\right)X+1$，所以

$$X^{2n}+1=\prod_{k=1}^{n}\left[X^2-\left(2\cos\frac{2k-1}{2n}\pi\right)X+1\right]. \tag{1}$$

2. $\mathbb{C}$ 上和 $\mathbb{R}$ 上的最简分式　现在，当我们知道了在 $\mathbb{C}$ 上和在 $\mathbb{R}$ 上既约多项式的一般形式之后，自然要回到最简分式 (第 5 章 §4 第 3 段) 的问题，因为这个问题在积分理论中是重要的．我们知道，首一既约多项式在 $\mathbb{C}$ 上形如 $X-c$，在 $\mathbb{R}$ 上形如 X^2+aX+b 或 $X-c$．因此，$\mathbb{C}$ 上的最简分式形如 $\dfrac{\gamma}{(X-c)^m}$,$\gamma\in\mathbb{C}$,$\mathbb{R}$ 上的最简分式除上述形式外，还要添加形如 $\dfrac{\alpha X+\beta}{(X^2+aX+b)^m}$ 的分式．当我们把真分式 $\dfrac{f}{g}$ 展开成 $\mathbb{C}$ 上或 $\mathbb{R}$ 上的最简分式之和时，如果分子 $g(X)$ 的典范展开式已知，方便的办法是 **待定系数法**. 我们通过一些例子阐述这个方法．

例 2　若 $g(X)=(X+1)^2(X^2+1)$ 是 $\mathbb{R}$ 上的典范展开式，那么对于分式 $\dfrac{1}{g(X)}$ 我们有

$$\frac{1}{(X+1)^2(X^2+1)}=\frac{\alpha}{(X+1)^2}+\frac{\beta}{X+1}+\frac{\gamma X+\delta}{X^2+1},$$

其中系数 $\alpha,\beta,\gamma,\delta\in\mathbb{R}$ 待定．用 $g(X)$ 乘此等式两边，得到

$$1=\alpha(X^2+1)+\beta(X+1)(X^2+1)+(\gamma X+\delta)(X+1)^2. \tag{*}$$

现在比较 $1,X,X^2,X^3$ 的系数，我们得一个有 4 个方程和 4 个未知数的非齐次线性方程组

$$\begin{aligned}
\alpha+\ \ \beta+\qquad\quad\ \ \delta&=1,\\
\beta+\ \ \gamma+\ \ 2\delta&=0,\\
\alpha+\ \ \beta+\ \ 2\gamma+\ \ \delta&=0,\\
\beta+\ \ \gamma\qquad&=0.
\end{aligned}$$

这个方程组自然是相容并且确定的，这可从第 5 章 §4 的定理 3 推出．解方程组，就得到结论

$$\frac{1}{(X+1)^2(X^2+1)}=\frac{1}{2(X+1)^2}+\frac{1}{2(X+1)}-\frac{X}{2(X^2+1)}.$$

更聪明的办法是，直接代入 X 的具体数值 $-1, i$ 到 $(*)$ 式中 $(-1, i$ 是既约因子的根). 立刻得到 $\alpha = \frac{1}{2}, (i\gamma + \delta)2i = 1$, 或 $\gamma = -\frac{1}{2}, \delta = 0$. 当 $X = 0$ 时就得到关于 β 的关系式.

例 3 设 $\deg f(X) < n, g(X) = (X - c_1)(X - c_2)\cdots(X - c_n)$, 其中 $c_1, c_2, \cdots, c_n$ 是 $\mathbb{C}$ 中或 $\mathbb{R}$ 中的两两不同的元素. 那么

$$\frac{f(X)}{(X - c_1)\cdots(X - c_n)} = \frac{\alpha_1}{X - c_1} + \cdots + \frac{\alpha_n}{X - c_n},$$

因此

$$f(X) = \sum_{k=1}^{n} \alpha_k (X - c_1)\cdots(X - c_{k-1})(X - c_{k+1})\cdots(X - c_n).$$

当 $X = c_k, 1 \leqslant k \leqslant n$ 时，有

$$f(c_k) = \alpha_k (c_k - c_1)\cdots(c_k - c_{k-1})(c_k - c_{k+1})\cdots(c_k - c_n),$$

而由于

$$g'(X) = \sum_{k=1}^{n} (X - c_1)\cdots(X - c_{k-1})(X - c_{k+1})\cdots(X - c_n),$$

所以

$$\alpha_k = \frac{f(c_k)}{g'(c_k)}, \qquad 1 \leqslant k \leqslant n.$$

结果得到 **拉格朗日公式**

$$\frac{f(X)}{g(X)} = \sum_{k=1}^{n} \frac{f(c_k)}{g'(c_k)(X - c_k)}, \tag{2}$$

它与 §1 的拉格朗日插值公式 (4) 有直接关系. 实际上，如果在 (2) 中用 $g(X)$ 乘两边并令 $f(c_k) = b_k$, 那么就得到 §1 的公式 (4).

在分式 $\frac{1}{g(X)}$ 中取 $g(X) = X^{2n} + 1$, 例 1 及公式 (2) 表明

$$\frac{1}{X^{2n} + 1} = -\frac{1}{2n} \sum_{k=1}^{2n} \frac{c_k}{X - c_k},$$

这是 $\mathbb{C}$ 上的最简分式展开，因为 $g'(X) = 2nX^{2n-1}, g'(c_k) = 2nc_k^{-1}c_k^{2n} = -2nc_k^{-1}$. 把含复共轭系数的被加项合并，我们就得到 $\mathbb{R}$ 上的最简分式展开：

$$\frac{1}{X^{2n} + 1} = -\frac{1}{2n} \sum_{k=1}^{n} \left(\frac{c_k}{X - c_k} + \frac{\bar{c}_k}{X - \bar{c}_k} \right) = \frac{1}{n} \sum_{k=1}^{n} \frac{1 - \left(\cos \frac{2k-1}{2n}\pi \right) X}{X^2 - \left(2\cos \frac{2k-1}{2n}\pi \right) X + 1}.$$

3. 多项式的隔根问题　我们把多项式 $f \in \mathbb{R}[X]$ 看作实变量 x 的实函数 $x \mapsto f(x)$, 并在平面直角坐标系 xOy 中画出此函数的图像. 多项式 $f(X)$ 的实根 (或说函数 $f(x)$ 的零点) 对应于图像与 x 轴的交点的横坐标 (图 25). 应该想到, 代数方程 $f(x) = 0$ 的根位于极值点之间 (或者恰在极值点处), 而极值点本身是更低次方程 $f'(x) = 0$ 的根.

实践中常常遇到的第一个问题, 是确定实根的界, 也就是说确定一个开区间 $a < x < b$, 使它含有所给多项式 f 的全体实根. 事实上, 从 §3 的引理 3 我们已经知道, 当 $|x| > \dfrac{A}{|a_0|} + 1$ 时 (a_0 是最高次项系数, $A = \max(|a_1|, \cdots, |a_n|)$) 函数 $f(x)$ 不取零值, 即使考虑复平面也是如此. 根的更精确的界在习题 1~4 中给出.

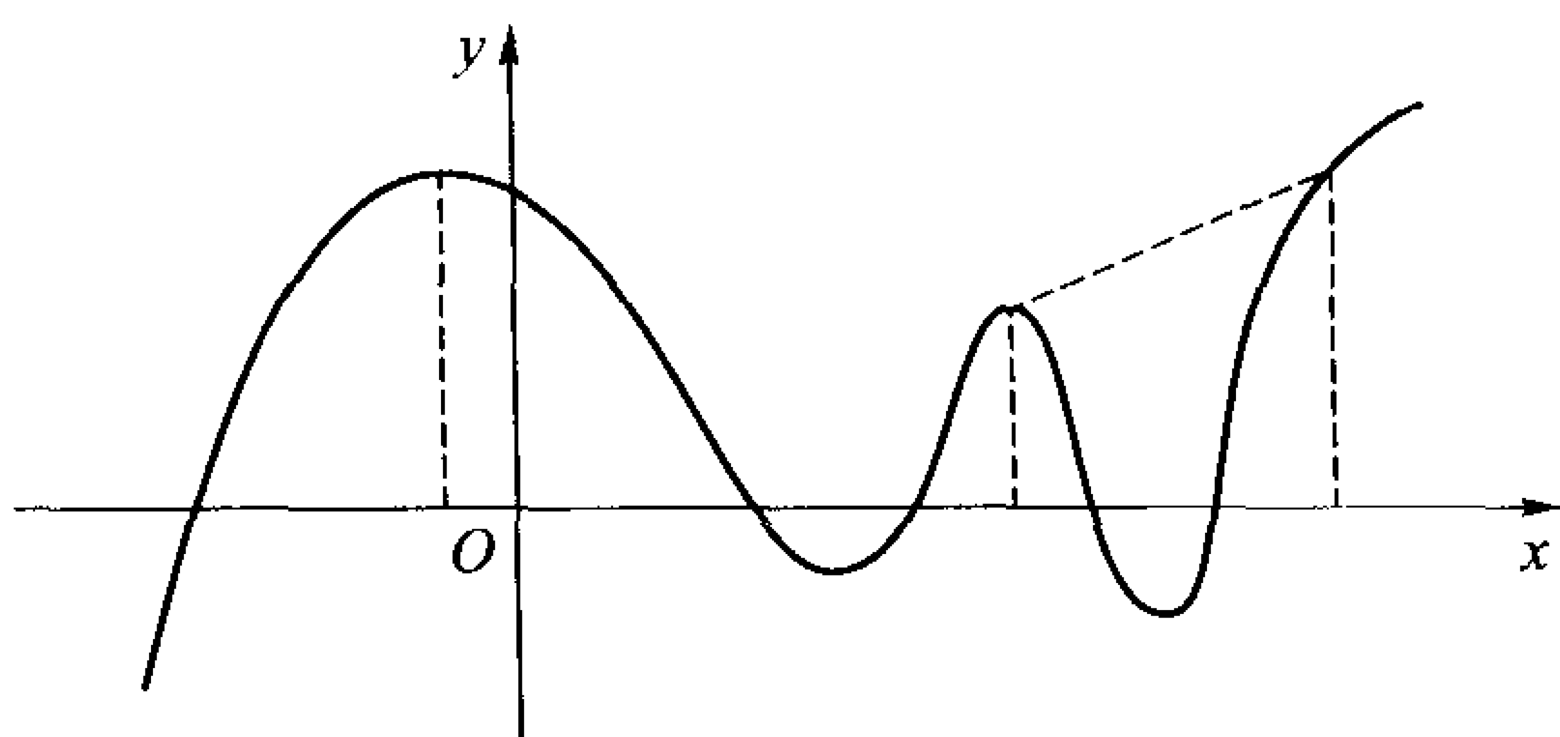


图 25

多项式的 **隔根**(或 **根的分离**) 的一般问题是这样提的: 对于每个实根, 指出一个仅含这一个实根而不含其他实根的开区间, 另一方面, 对于每个开区间, 指出含在此区间内的实根的个数.

对这个问题的最早的令人满意的解答是斯图姆 1829 年给出的, 尽管有点不精巧. 在叙述相应的定理及其证明之前先引入一些必要的定义.

定义 1　设 $S = \{c_1, \cdots, c_m\}$ 是一个非零实数的有限序列, 并设 $V(S)$ 是使 $c_i c_{i+1} < 0$ 的脚标 $i, 1 \leqslant i \leqslant m-1$, 的数目. 那么 $V(S)$ 叫作数列 S 中的变号数. 如果数列 S 含有零, 则把 $V(S)$ 理解为从 S 中删除零后得到的数列 S' 中的变号数.

例如, $V(\{1, 0, 2, 0, -3, 4, 0, 0, -2\}) = 3$. 今后, 不失一般性总假定我们所讨论的实系数多项式没有重根, 这件事 (见 §1 第 4 段末) 总是可以办到的.

定义 2　非零实系数多项式的有限序列

$$f_0(x) = f(x),\ f_1(x),\ \cdots,\ f_s(x) \tag{3}$$

叫作关于多项式 $f(x)$ 在闭区间 $[a, b]$ $(a \leqslant x \leqslant b)$ 上的 **斯图姆组**(或 **斯图姆序列**), 如果下述条件成立:

i) 最后一个多项式 $f_s(X)$ 在 $[a, b]$ 上没有根;

ii) $f_0(a) f_0(b) \neq 0$;

iii) 若对于 $c \in [a, b]$ 和 $1 \leqslant k \leqslant s-1$, $f_k(c) = 0$ 则 $f_{k-1}(c) f_{k+1}(c) < 0$;

iv) 若对于 $c\in[a,b]f(c)=0$, 则乘积 $f_0(x)f_1(x)$ 当 x 递增经过点 c 时从负号变到正号. 换言之, 存在 $\delta>0$, 使得 $x\in(c-\delta,c)$ 时, $f_0(x)f_1(x)<0$ 而 $x\in(c,c+\delta)$ 时 $f_0(x)f_1(x)>0$.

我们指出斯图姆组 (3) 的相邻多项式在 $[a,b]$ 上没有共同的根: 如果 $f_{k-1}(c)=f_k(c)=0, k\geqslant 1$, 那么 $f_{k-1}(c)f_{k+1}(c)=0$, 与条件 iii) 矛盾.

为简单起见, 记

$$V_c=V_c(f)=V(\{f_0(c),f_1(c),\cdots,f_s(c)\}),\quad c\in[a,b].$$

定理 2(斯图姆) *次数 $n\geqslant 1$ 的实多项式 $f(x)$ 在开区间 (a,b) 上的根的数目等于差 V_a-V_b, 其中 V_a,V_b 对应于任一固定的斯图姆组 (3).*

证明 斯图姆组 (3) 的多项式在 $[a,b]$ 中的相异实根的全体把闭区间 $[a,b]$ 分成一些子开区间 (a_j,a_{j+1}), 满足 $a=a_0<a_1<\cdots<a_m=b$, 在这些子开区间中任何多项式 $f_i, 0\leqslant i\leqslant s$ 都没有根. 我们将比较对应于不同的点 $c\in(a_j,a_{j+1})$ 的值 V_c.

开始取 $c\in(a_0,a_1)$, 那么 $f_0,\cdots,f_s$ 在 (a_0,c) 中都没有根. 根据波尔查诺–柯西中间值定理, $f_i(a_0)f_i(c)\geqslant 0, 0\leqslant i\leqslant s$. 当对于一切 $i f_i(c)\neq 0$ 时有 $f_i(a_0)f_i(c)>0$, 由此推出 $V_{a_0}=V_c$. 如果对于某个 $k f_k(a_0)=0$, 则根据斯图姆组的性质 i),ii) 必有 $k\neq 0,s$. 根据性质 iii), 我们有 $f_{k-1}(a_0)f_{k+1}(a_0)<0$. 同时, $f_{k-1}(x)$ 和 $f_{k+1}(x)$ 在 (a_0,c) 中没有根, 所以由波尔查诺–柯西定理, $f_{k-1}(a_0)f_{k-1}(c)>0$ 且 $f_{k+1}(a_0)f_{k+1}(c)>0$. 这表明 $f_{k-1}(c)f_{k+1}(c)<0$. 我们得到下述结论, 在计算 V_{a_0} 和 V_c 时, 子序列 $f_{k-1}(a_0),0,f_{k+1}(a_0)$ 和 $f_{k-1}(c),f_k(c),f_{k+1}(c)$ 不依赖于 $f_k(c)$ 的值而具有同样的作用 (都给出一次变号). 这件事对于一切使 $f_k(a_0)=0$ 的 k 成立, 因此 $V_{a_0}=V_c$. 类似的讨论适用于另一个边缘开区间中的点:

$$c\in(a_{m-1},a_m)\Rightarrow V_c=V_{a_m}.$$

现在设 $c\in(a_{j-1},a_j)$,$c'\in(a_j,a_{j+1})$ 是两个相邻的开区间中的点, $1<j<m-1$(图 26). 与上述相同的讨论指出, 如果 $f(a_j)\neq 0, V_c=V_{c'}$.

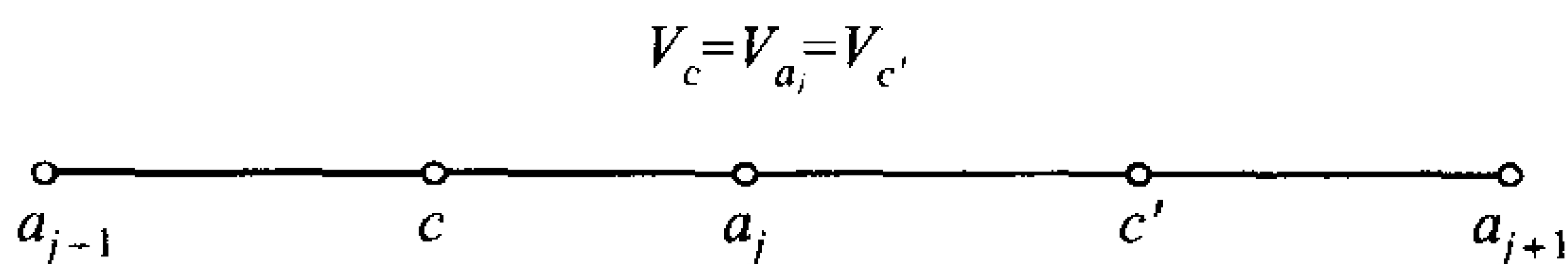


图 26

在 $f_0(a_j)=f(a_j)=0$ 的情况下, 第一次出现差别. 事实上, 根据条件 iv) 我们有 $f_0(c)f_1(c)<0$ 和 $f_0(c')f_1(c')>0$, 即在子序列 $f_0(c),f_1(c)$ 中有一次变号而在子序列 $f_0(c'),f_1(c')$ 中无变号. 同时, 我们前面的讨论表明, 对于 $k>1$, 在子序列 $f_{k-1}(c),f_k(c),f_{k+1}(c)$ 和 $f_{k-1}(c'),f_k(c'),f_{k+1}(c')$ 中的变号数是一样的, 于是若 $f(a_j)=0$, 则 $V_c-V_{c'}=1$.

固定点 $c_k \in (a_{k-1}, a_k), 1 \leqslant k \leqslant m$, 并写出恒等式

$$V_a - V_b = (V_a - V_{c_1}) + \sum_{k=1}^{m-1}(V_{c_k} - V_{c_{k+1}}) + (V_{c_m} - V_b).$$

已知两端括号中的表达式等于零，同时

$$V_{c_k} - V_{c_{k+1}} = \begin{cases} 0, & 若 f(a_k) \neq 0, \\ 1, & 若 f(a_k) = 0. \end{cases}$$

在闭区间 $[a, b]$ 中多项式 $f(x)$ 没有其他的根 (根据结构，斯图姆组的多项式的全部根都落在点 $a_0, a_1, \cdots, a_m$ 上). 求和之后得知差 $V_a - V_b$ 等于多项式 $f(x)$ 在开区间 (a, b) 内的根的数目. □

为了应用所证的定理，必须学会对于每个具体的实多项式 $f(x)$ 构作斯图姆组. 最常用的是 **标准斯图姆组**, 它可用我们在第 5 章中学会的欧几里得算法稍加改变得到. 即在第 5 章 §3 中的序列 (5) 中，从 $f_0(x) = f(x), f_1(x) = f'(x)$(多项式的导数) 开始，逐次取余式并冠以相反符号作为该组的多项式. 准确地说，令

$$\begin{gathered} f_0(x) = f(x), f_1(x) = f'(x); \\ f_0(x) = q_1(x)f_1(x) - f_2(x), \quad \deg f_2 < \deg f_1; \\ \cdots\cdots\cdots\cdots \\ f_{k-1}(x) = q_k(x)f_k(x) - f_{k+1}(x), \quad \deg f_{k+1} < \deg f_k; \\ \cdots\cdots\cdots\cdots \\ f_{s-1}(x) = q_s(x)f_s(x). \end{gathered} \tag{4}$$

根据定义 $f_s(x) = \text{g.c.d.}(f, f')$ 是非零常数，因为我们假设 $f(x)$ 没有重根 (如果我们事先不知道这一点，则在得到函数组 (4) 之后将其转换为 $g_k(x) = \dfrac{f_k(x)}{f_s(x)}, 0 \leqslant k \leqslant s$.)

定理 3 上述构作的函数组

$$f_0(x) = f(x), \quad f_1(x) = f'(x), \quad f_2(x), \quad \cdots, \quad f_s(x) \tag{5}$$

是斯图姆组.

证明 根据假定, 性质 ii) 成立, 而性质 i) 从 $f_s(x) = \text{const} \neq 0$ 推出. 若 $f_k(c) = 0$, 则从 (4) 可见， $f_{k-1}(c)f_{k+1}(c) \leqslant 0$ 并且 $f_{k+1}(c) = 0$ 当且仅当 $f_{k-1}(c) = 0$. 而若是如此，则 $0 = f_{k-1}(c) = f_k(c) = f_{k+1}(c) = f_{k+2}(c) = \cdots$ 与 $f_s(c) \neq 0$ 矛盾. 于是 $f_{k-1}(c)f_{k+1}(c) < 0$, 得到性质 iii). 最后，假定对于某点 $c \in [a, b], f_0(c) = 0$. 那么 $f_0(x) = (x - c)q(x), q(c) \neq 0$ 且 $f_0(x)f_1(x) = (x - c)[q^2(x) + (x - c)q(x)q'(x)] = (x - c)g(x)$, 其中 $g(x) = q^2(x) + (x - c)q(x)q'(x)$. 我们有 $g(c) = q^2(c) > 0$, 从而在点 c 的小邻域 $(c - \delta, c + \delta)$ 上 $g(x)$ 取正值. 这时乘积 $f_0(x)f_1(x)$ 与因子 $x - c$ 一样，当点 x 递增经过 c 时，从负号变为正号. 于是，函数组 (5) 具有性质 iv). □

注记 1 由函数组 (5) 逐项乘以正的常数 $\lambda_0, \lambda_1, \cdots, \lambda_s$ 得到的函数组

$$\lambda_0 f_0(x), \quad \lambda_1 f_1(x), \quad \cdots, \quad \lambda_s f_s(x) \tag{5'}$$

也是斯图姆组. 我们把它叫作几乎标准斯图姆组. 这种斯图姆组对于计算有用.

注记 2 $f(x)$ 没有重根的条件对于不同实根的数目是非本质的, 如标准斯图姆组的构造所示, 可以把 $f_k(x)$ 转换为 $g_k(x) = \dfrac{f_u(x)}{f_s(x)}$, 并注意到 $V_c(g) = V_c(f)$.

注记 3 根据 §3 的引理 3, 对于斯图姆组的每个多项式 $f_i(x)$ 都存在这样一个数 r_i, 使得此多项式的全部实根都落在 $-r_i$ 和 r_i 之间. 设 M 是任意一个足够大的数, 譬如设 $M = \max\limits_{0 \leqslant i \leqslant s} r_i$. 那么每个多项式 $f_i(x) = a_{(i)}x^{k_i} + \cdots$ 的实根都分布在 $-M$ 和 M 之间, 不仅如此, 当 $x = M$ 时 $f_i(M)$ 的符号与它的最高次项 $a_{(i)}M^{k_i}$ 的符号一致. M 的具体值对于我们的程序也不是本质的, 因此在求多项式 $f(x)$ 的相异实根的总数时, 我们常常象征性地假定 $x = -M$ 和 $x = M$.

注记 4 据说, 斯图姆本人常常这样来表达对于自己 (确实卓越的) 成就的自豪感, 在给学生讲述了证明之后补充道 "这就是以我的名字命名的定理".

我们来看几个例子.

例 4 $f(x) = x^3 + 3x - 1$. 首先, $f_1(x) = f'(x) = 3x^2 + 3$; 然后, $f(x) = (3x^2 + 3)\dfrac{1}{3}x + 2x - 1$, 于是 $f_2(x) = -2x + 1$; $3x^2 + 3 = (-2x + 1)\left(-\dfrac{3}{2}x - \dfrac{3}{4}\right) + \dfrac{15}{4}$, 从而 $f_3(x) = -\dfrac{15}{4}$. 根据注记 1, 可取 $x^3 + 3x - 1, x^2 + 1, -2x + 1, -1$ 为斯图姆组. 编制最高次项符号的表格

	x^3	$3x^2$	$-2x$	-1	V
$x = -M$	$-$	$+$	$+$	$-$	2
$x = M$	$+$	$+$	$-$	$-$	1

我们得到 $V_{-M} - V_M = 1$, 即 $x^3 + 3x - 1$ 有一个实根.

例 5 $f(x) = x^3 + 3x^2 - 1$. 易见, $f(x)$ 具有形如 $x^3 + 3x^2 - 1, 3x^2 + 6x, 2x + 1, 1$ 的标准斯图姆组, 而最高次项的符号表是

	x^3	$3x^2$	$2x$	1	V
$x = -M$	$-$	$+$	$-$	$+$	3
$x = M$	$+$	$+$	$+$	$+$	0

我们得到结论, $f(x)$ 有三个实根: $V_{-M} - V_M = 3$.

例 6 $f(x) = 1 + x + \dfrac{1}{2!}x^2 + \cdots + \dfrac{1}{n!}x^n$(**截断指数函数**). 显然, 此多项式若有实根, 必位于 $(-M, -\delta)$ 之内, 其中 $\delta > 0$ 是充分小的实数 (M 永远被认为是充分大的正数). 可以取三个多项式 $f_0(x) = f(x), f_1(x) = f'(x) = 1 + x + \dfrac{1}{2!}x^2 + \cdots + \dfrac{1}{(n-1)!}x^{n-1}$ 和 $-\dfrac{1}{n!}x^n = -f(x) + f'(x)$ 为闭区间 $[-M, -\delta]$ 上的非标准斯图姆组 (验证性质 i)~iv)

成立). 从符号表

	f_0	f_1	f_2	V
$-M$	$(-1)^n$	$(-1)^{n-1}$	$(-1)^{n-1}$	1
δ	+	+	$(-1)^{n-1}$	$\frac{1+(-1)^n}{2}$

看到，对于偶数 $n, f(x)$ 没有实根，而当 n 为奇数时有一个负根 (易见，此根随着 $n=2m+1$ 的增加而趋于 $-\infty$).

例 7 $f(x)=x^3+px+q$. 可取 $f_0=f, f_1=3x^2+p, f_2=-2px-3q, f_3=-4p^3-27q^2$ 为任何一个使得 $f(a)f(b)\neq 0$ 的闭区间 $[a,b]$ 上的几乎标准斯图姆组 (参见注 1). 其中 $f_3=D(f)$ 是多项式 f 的判别式 (见 §2 的 (16), 其中把 a 和 b 换成更常用的系数 p 和 q). 根据一般原理，$f(x)$ 要么有一个实根，要么有三个实根. 如果考虑到数对 $(\mathrm{sgn}p, \mathrm{sgn}D(f))$ 的三种变化，注意 $p\geqslant 0 \Rightarrow D(f)\leqslant 0$, 那么从符号表

	x^3	x^2	$-2px$	$D(f)$
$-M$	$-$	+	$\mathrm{sgn}p$	$\mathrm{sgn}D(f)$
M	+	+	$-\mathrm{sgn}p$	$\mathrm{sgn}D(f)$

易见：当 $D(f)<0$ 时，f 有一个实根而当 $D(f)>0$ 时，f 有三个实根.

4. 只有实根的实多项式 我们再来考虑一个在实际应用中很重要的情况，即根据某种理由知道多项式 $f(x)=\sum\limits_{k=0}^{n}a_kx^{n-k}\in\mathbb{R}[x]$ 的根全都是实数，为方便起见，引入两个记号：

$m(f)$—— 多项式 f 的正根的数目 (按重数计算);

$W(f)=V(\{a_0,a_1,\cdots,a_n\})$—— 多项式 f 的系数序列的变号数.

显然，$0\leqslant W(f)\leqslant n=\deg f$, 而且 $W(-f)=W(f)$. 我们还指出 $W(f)=W(aX^k+a_{i_1}X^{n-i_1}+\cdots)$ (其中指数 k 满足唯一的条件 $k>n-i_1$(系数 $a_1,\cdots,a_{i_1-1}$ 都是零) 且 $aa_0>0$. 如果 $W(f)=0$, 那么 f 没有正根. 另一方面，当 $W(f)=\deg f$ 时，f 也可能没有正根，例子是：$f(X)=X^2-X+1$. 然而，我们将看到，$W(f)$ 与多项式 f 的正根数目有直接关系. 例如，笛卡儿符号法则：$W(f)\geqslant m(f)$ 成立，并且 $m(f)=W(f)(\mathrm{mod}2)$. 我们不证明这个法则，而转向我们感兴趣的情况.

定理 4 *如果多项式 $f\in\mathbb{R}[X]$ 的全部根都是实根. 则 $m(f)=W(f)$.*

证明 从直观出发, 根据分析学中著名的罗尔定理 (或中值定理), 在多项式 $f(X)$ 的根 a' 和 b' 之间，存在数 $c\in\mathbb{R}$,$a'<c<b'$, 使得 $f'(c)=0$. 由此推出，导函数 $f'(X)$ 的所有的根都是实的并且 $m(f')=m(f)$ 或者 $m(f')=m(f)-1$.

事实上，设 $c_1<c_2<\cdots<c_r$ 是多项式 f 的重数为 $n_1,n_2,\cdots,n_r$ 的根，那么 $n_1+n_2+\cdots+n_r=\deg f=n$. 根据 §1 定理 5, 导数 f' 有重数为n_1-1, $n_2-1,\cdots,n_r-1$ 的根 $c_1,c_2,\cdots,c_r$, 而根据罗尔定理，在 f 的相邻两根之间，还有

导数 f' 的根 $c_1', c_2', \cdots, c_{r-1}'$. 总共得到 $(n_1-1)+\cdots+(n_r-1)+r-1=n-1$ 个实根. 由于 $\deg f'=n-1$, 所以 f' 没有其他的根.

其次, 设 $c_{l-1}<0$ 而 $c_l, \cdots, c_r$ 是重数为 $n_l, \cdots, n_r$ 的全体正根: $n_l+\cdots+n_r=m=m(f)$. 重数为 $n_l-1, \cdots, n_r-1$ 的根 $c_l, \cdots, c_r$, 和根 $c_l', \cdots, c_{r-1}'$, 可能还有 c_{l-1}' 就是 $f'(X)$ 的全部正根, 其总数为 $m(f')=m(f)-1$ 或 $m(f)$, 这就证明了上述断言. 这个事实的解析表达式如下:

$$m(f)=m(f')+\varepsilon, \quad \varepsilon=\frac{1}{2}(1-(-1)^{m(f)+m(f')}). \tag{6}$$

我们还要指出, 如果

$$f(X)=a_0X^n+\cdots+a_{n-\nu}X^{\nu}, \tag{7}$$

其中 $a_{n-\nu}$ 是最后一个非零系数, 那么

$$f(X)=(X-c_l)^{n_l}\cdots(X-c_r)^{n_r}g(X).$$

其中

$$g(X)=a_0X^{n-m}+\cdots+bX^{\nu}, \quad a_0>0, b>0(\nu\geqslant 0).$$

于是 $a_{n-\nu}=(-1)^m c_l^{n_l}\cdots c_r^{n_r}b$, 并且 $c_l^{n_l}\cdots c_r^{n_r}b>0$. 换言之

$$(-1)^{m(f)}a_{n-\nu}>0. \tag{8}$$

当 $n=1,2$ 时, 定理的结论是明显的. 现对 $n=\deg f$ 作归纳, 假设定理对于一切次数 $<n$ 的多项式成立. 若在 (7) 中 $\nu>0$, 即 $a_n=0$, 那么 $f(X)=Xf_1(X)$, 且 $m(f)=m(f_1)=W(f)$(根据归纳假设 $m(f_1)=W(f_1)$). 剩下的是考虑 $a_n\neq 0$ 的情形. 设

$$f'(X)=na_0X^{n-1}+\cdots+\mu a_{n-\mu}X^{\mu-1}, \quad a_{n-\mu}\neq 0.$$

那么

$$W(f)=W(f')+\delta, \quad \delta=\frac{1}{2}\left(1-\frac{a_na_{n-\mu}}{|a_na_{n-\mu}|}\right)=0\text{或}1.$$

但我们知道 (见 (8)), $(-1)^{m(f)}a_n>0$ 且 $(-1)^{m(f')}a_{n-\mu}>0$. 因此 $\delta=\frac{1}{2}(1-(-1)^{m(f)+m(f')})$, 从而 $\delta=\varepsilon$. 根据归纳假定 $W(f')=m(f')$, 所以 $W(f)=m(f')+\varepsilon$, 与 (6) 比较, 得到 $m(f)=W(f)$. □

推论(比丹－傅里叶定理的特殊情形)　设多项式 f 的根都是实根. 那么位于开区间 (a,b) 内的根的数目等于 $W(f_a)-W(f_b)$, 其中

$$f_a(X)=f(X+a)=\sum_{k=0}^{n}\frac{1}{k!}f^{(k)}(a)X^k,$$

$$f_b(X)=f(X+b)=\sum_{k=0}^{n}\frac{1}{k!}f^{(k)}(b)X^k.$$

是泰勒级数展开式 (见习题 3).

证明　根据定义, 多项式 f_a 的正根数目 $m(f_a)$ 等于多项式 f 的大于 a 的根的数目. 关于 f_b 有同样的说法. 因此, 多项式 f 的包含在 a 和 b 之间 $(a<b)$ 的根的数目等于 $m(f_a)-m(f_b)$, 根据定理 3, 它等于 $W(f_a)-W(f_b)$. □

5. 稳定多项式　实系数首一多项式

$$f(X)=X^n+a_1X^{n-1}+\cdots+a_{n-1}X+a_n$$

叫作**稳定的**, 如果它的根全都位于左半平面中 (图 27):

$$f(\lambda)=0,\quad \lambda=\alpha+i\beta\Longrightarrow\alpha<0.$$

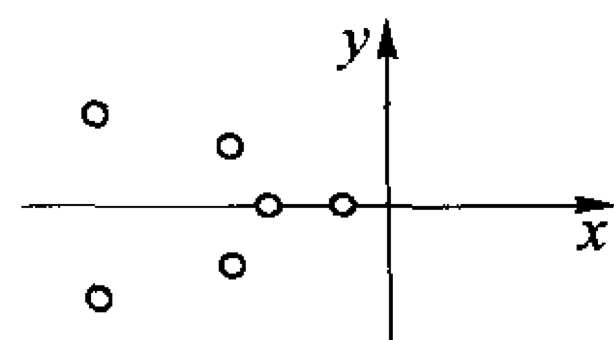


图 27

这个术语来源于微分方程论. 在微分方程论中有一个物理系统 (可以更广泛地理解为力学的、技术的或经济的系统), 它在平衡位置附近是渐近稳定的, 要求

$$\lim_{t\to+\infty}e^{\lambda t}=0\tag{9}$$

其中 $\lambda=\alpha+i\beta(\alpha,\beta\in\mathbb{R})$ 是与 n 阶常系数微分方程相关的多项式的任意根. 按照欧拉公式 (见第 5 章 §1(15)) $e^{\lambda t}=e^{\alpha t}e^{i\beta t}=e^{\alpha t}(\cos\beta t+i\sin\beta t)$, 所以控制项是 $e^{\alpha t}$, 从而条件 (9) 等价于不等式 $\alpha<0$.

这就引出了一类特殊的局部化问题——劳思－胡尔维茨 (Routh-Hurwitz) 问题[①]: 必须直接根据多项式 f 的系数, 判断它是不是稳定的. 这个代数问题早在 1895 年被劳思－胡尔维茨解决, 他们给出的判别准则如下.

多项式 f 是稳定的, 当且仅当下述不等式成立:

$$\Gamma_1>0,\Gamma_2>0,\cdots,\Gamma_n>0,\tag{10}$$

①此问题实际上更早 (1868 年) 由美国物理学家 D.K. 麦克斯韦提出, 并且在次数不高的情况下被俄罗斯工程师 N.A. 维施涅格拉茨基所解决, 他曾在 1876 年研究了调节器的稳定性问题.

其中

$$\Gamma_k = \begin{vmatrix} a_1 & 1 & 0 & 0 & 0 & 0 & \cdots & 0 \\ a_3 & a_2 & a_1 & 1 & 0 & 0 & \cdots & 0 \\ a_5 & a_4 & a_3 & a_2 & a_1 & 1 & \cdots & 0 \\ a_7 & a_6 & a_5 & a_4 & a_3 & a_2 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ a_{2k-1} & a_{2k-2} & a_{2k-3} & a_{2k-4} & a_{2k-5} & a_{2k-6} & \cdots & a_k \end{vmatrix}$$

(假定当 $s > n$ 时 $a_s = 0$).

我们不打算证明劳思 - 胡尔维茨定理 (这件事更适于在其他课程中进行), 而是注意到这个优美的定理完全依赖于行列式理论.

其次, 根据定理 1, 当条件 (10) 成立时, 多项式 $f(X)$ 被表示成形如 $X+u, X^2+vX+w$ 的因式的乘积, 其中 $u>0, v>0, w>0$, 这就意味着稳定多项式 $f(X)$ 的所有系数都是正的:

$$a_1 > 0,\ a_2 > 0,\ \cdots,\ a_n > 0. \tag{11}$$

于是, 条件 (11) 对于多项式 $f(X)$ 的稳定性是必要的. 在一般情况下这些条件不是充分的, 但却能把 (10) 中行列式不等式的数目大约减少一半. 这是很有价值的, 因为计算行列式可是个累活.

例 8 当 $n=2$ 时, 不等式组 $\Gamma_1>0, \Gamma_2>0$ 与更简单的不等式组 $a_1>0, a_2>0$ 等价, 这从二次方程的求根公式顺便看出.

当 $n=3$ 时, 由于 $\Gamma_3 = a_3(a_1a_2 - a_3)$, 判别准则归结为不等式 $a_1>0, a_2>0, a_3>0, a_1a_2>a_3$.

最后我们指出, 劳斯 - 胡尔维茨准则并未解决与稳定性相关的全部问题, 因为在实际应用中要遇到系数依赖于参数的微分方程和多项式. 用参数的语言来叙述稳定性条件乃是性质完全不同的另一个问题.

6. 多项式的根对系数的依赖关系 很明显, 多项式的根是它的系数的函数. 现在我们着重指出, 这些函数是连续的, 也就是说, *当系数的改变充分小时, 根的改变小得可以忽略*. 可是, 多重根却可以分裂, 而且所发生的变化在几何上常常具有奇怪的形式, 只要比较一下多项式 z^n 和 $z^n+\varepsilon$ 当 $\varepsilon \to 0$ 时的状态, 就可以看到这种复杂性了. 下述定理有助对多项式作出质的和量的比较.

定理 5(鲁歇 Rouché) *设 $f_0(z)$ 和 $f_1(z)$ 是两个多项式, 如果不等式*

$$|f_1(z)| < |f_0(z)|$$

对于有界闭区域 $D \subset \mathbb{C}$ 中的一切 z 都成立, 那么多项式 $f_0(z)+f_1(z)$ 在 D 内与 $f_0(z)$ 有同样多的根.

这个定理的证明可以在更一般的背景下, 借助复变函数论的初等工具得到, 我们在这里略去. □

现设 z_0 是多项式 $f_0(z)=a_0z^n+a_1z^{n-1}+\cdots+a_n$ 的 k 重根. 我们来考察多项式

$$f(z)=(a_0+\delta_0)z^n+(a_1+\delta_1)z^{n-1}+\cdots+(a_n+\delta_n)=f_0(z)+f_1(z)$$

其中 $|\delta_i|<\delta,\delta$ 是一个相当小的实数. 考虑圆 $D=\{z\in\mathbb{C}\,\big|\,|z-z_0|\leqslant\varepsilon\}$, 它以 z_0 为中心以一个相当小的 $\varepsilon>0$ 为半径, 使得 z_0 是多项式 $f_0(z)$ 在闭区域 D 内的唯一的根. 函数 $|f_0(z)|$ 是连续的并且在圆周 $|z-z_0|=\varepsilon$—— 圆 D 的边界上不等于零, 因此 $\mu=\inf\limits_{|z-z_0|=\varepsilon}|f_0(z)|>0$. 取 δ 充分小, 使得当 $|z-z_0|=\varepsilon$ 时有不等式 $|f_1(z)|<\mu$. 那么鲁歇定理的条件满足, 从而 $f(z)$ 和 $f_0(z)$ 在 D 内同有 k 个根. 特别地, 单根 $(k=1)$ 在系数的微小变动之下依然是单根, 只是小有位移.

我们事实上已经做出了多项式 $f(z)$ 的根的局部化, 它保证了这些根连续依赖于多项式 $f_0(z)$ 的系数.

所得结果可以叙述成下述形式.

定理 6　设 $f_0(z)=z^n+a_1z^{n-1}+\cdots+a_n$ 是首一复多项式, $c_1,\cdots,c_n$ 是它的根. 对于任意的 $\varepsilon\in\mathbb{R},\varepsilon>0$, 存在 $\delta\in\mathbb{R},\delta>0$, 使得对于每个满足条件 $|a'_j-a_j|<\delta,1\leqslant j\leqslant n$, 的首一多项式 $f(z)=z^n+a'_1z^{n-1}+\cdots+a'_n$ 都有展开式 $f(z)=\prod\limits_{j=1}^{n}(z-c'_j)$ 并且 $|c'_j-c_j|<\varepsilon,\quad 1\leqslant j\leqslant n.$

这个定理也可以不用鲁歇定理证明 (例如: 见 Amer.Math.Monthly,1989,V.96,No.4), 然而对于我们来说, 更重要的是注意到事情的本质.

7. 多项式根的计算　局部化问题的完全解决 (特别是如果考虑全部复根的话, 那就不能只谈开区间而必须谈平面 $\mathbb{C}$ 的区域) 是以高昂的代价实现的. 我们在本段中简略地叙述 "局部化根" 的具有给定精确度的数值计算.

设已知实轴上的一个小开区间 (a,b) 含有多项式 $f(x)$ 的唯一一个我们感兴趣的单根 c. 那么 $f(a)f(b)<0$. 把开区间 (a,b) 分成十等份. 这十份之中的一个 (且仅有一个)$(a_1,b_1)\subset(a,b)$, 具有性质 $f(a_1)f(b_1)<0$. 这表明 $c\in(a_1,b_1)$. 再把 (a_1,b_1) 十等分并选出其中的一个 $(a_2,b_2)\subset(a_1,b_1)$ 使 $f(a_2)f(b_2)<0$. 由于 $c\in(a_2,b_2)$, 那么这个步骤还可继续下去, 于是得到根 c 的精确到 $0.1,0.01$, 等等的近似值. 这种试验方法 (若十等分开区间即为十进的, 若二等分开区间则为二进的) 是实用的, 如果我们不期望得到很高的精确度并且只有最简单的计算工具的话.

罗巴切夫斯基方法是一个通用的方法, 但也是十分笨重的方法. 它可以同时求出包括复根在内的一切根的近似值, 并且不需要预先将这些根隔离开.

线性插值法 (或 **伪位置法**) 得到了广泛的传播. 此方法可如下进行, 作为根的近似值的 $c_{(1)}$, 把开区间 (a,b) 分成等于 $|f(a)|$ 和 $|f(b)|$ 的比的两部分. 换言之,

$$\frac{c_{(1)}-a}{b-c_{(1)}}=-\frac{f(a)}{f(b)},\quad c_{(1)}=\frac{bf(a)-af(b)}{f(a)-f(b)}.$$

曲线 $y=f(x)$ 在区间 (a,b) 上的一小段用弦来表示 (图 28).

重复这一步骤, 类似地得到近似值 $c_{(2)}$, 等等.

我们再来介绍一种方法. 在根 c 的充分小的邻域 (a,b) 中, 曲线段可以用一点处的切线段代替. 如果 c_0 是对于根的某个近似 (在图 28 上 $c_0=a$), 那么根据拉格朗日有限增量定理, 我们有

$$f(x)-f(c_0)=f'(c_0)(x-c_0),$$

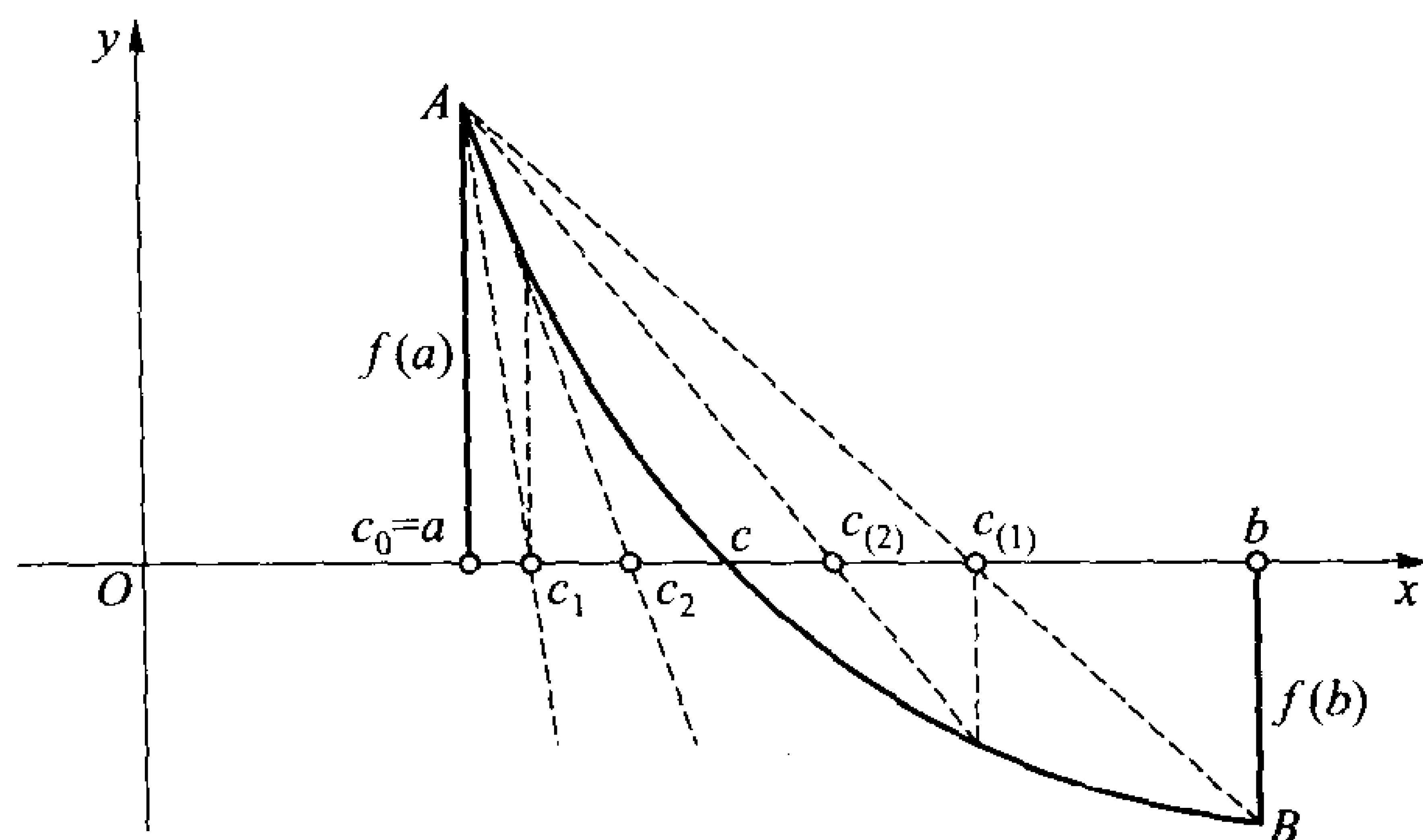


图 28

因此对于 $x=c$ 我们得到 $0=f(c)=f(c_0)+f'(c_0)(c-c_0)$. 因此作为下一个近似值自然取 $c_1=c_0-\dfrac{f(c_0)}{f'(c_0)}$. 令

$$c_{k+1}=c_k-\frac{f(c_k)}{f'(c_k)},\quad k=0,1,2,\cdots, \tag{12}$$

如果递归序列 (12) 收敛, 也就是说, 当 $k\to\infty$ 时 $c_k\to\bar{c}$, 我们就得到 $\bar{c}=\bar{c}-\dfrac{f(\bar{c})}{f'(\bar{c})}$, 即 $f(\bar{c})=0$. 只要出发点 c_0 取得恰当, 序列的一切点都落在开区间 (a,b) 中, 且 $c=\bar{c}$. 图 28 只表示了前两个导函数 $f'(x), f''(x)$ 在开区间 (a,b) 中的四种可能性状中的一种. 我们省略细节, 请读者自己去考虑余下的情形.

刚才描述的方法称为 **牛顿法**, 是一种最常用的且收敛迅速的方法. 初等的分析方法表明, 若当 $x\in[a,b]$ 时

$$|f(x)|\geqslant M_1,\quad |f''(x)|\leqslant M_2$$

则 $|c_1-c|\leqslant\dfrac{M_2}{2M_1}|c_0-c|^2$. 因此, 只要选择点 c_0 使得

$$\frac{M_2}{2M_1}|c_0-c|\leqslant q<1,$$

我们就得到估计式 $\frac{M_2}{2M_1}|c_k - c| \leqslant q^{2^k}$. 如常所述，这是逼近根 c 的 **平方收敛** (或 **超指数收敛**). 牛顿法的好处还在于它无需改变就适用于计算 $\mathbb{C}[z]$ 中多项式的任意复根. 其中递归序列 (12) 是计算的基础.

当然，我们仅限于对计算方法框架作一个大略的描述而没有涉及实际的计算结构. 现代计算数学为此提供了大量的工具. 我们不可能涉及数学计算人员专业的细致工作.

8. 整系数多项式的有理根 关于 $\mathbb{Q}$ 上和 $\mathbb{Z}$ 上的多项式，我们在第 5 章 §3 的第 4 段已经能够讨论了，特别是将 $\mathbb{Q}$ 上给定的多项式分解成既约因式的问题. 现在我们来看远为简单的关于多项式 $f \in \mathbb{Q}[X]$ 的有理线性因子的分解问题，实际上也就是有理根的问题. 将 f 乘以系数的公分母，我们就将 f 转换成 $\mathbb{Z}[X]$ 上的多项式，因此从一开始就可以只考虑整系数多项式.

定理 7 设某分数 $\frac{p}{q}$ 是多项式 $f(X) = a_0X^n + a_1X^{n-1} + \cdots + a_n \in \mathbb{Z}[X]$ 的根，$a_0a_n \neq 0$. 那么 $p|a_n$ 且 $q|a_0$.

证明 实际上，根据条件

$$a_0\left(\frac{p}{q}\right)^n + a_1\left(\frac{p}{q}\right)^{n-1} + \cdots + a_{n-1}\frac{p}{q} + a_n = 0.$$

以 q^n 乘等式的两边，我们得到

$$a_0p^n + a_1p^{n-1}q + \cdots + a_{n-1}pq^{n-1} + a_nq^n = 0,$$

$$a_0p^n = q(-a_1p^{n-1} - \cdots - a_{n-1}p^{n-2} - a_nq^{n-1}).$$

于是， $q|a_0p^n$, 而由于 q 和 p 互素，所以 $q|a_0$. 类似地，从等式

$$a_nq^n = p(-a_0p^{n-1} - \cdots - a_{n-2}pq^{n-2} - a_{n-1}q^{n-1})$$

推出 $p|a_n$. □

推论 首一多项式的有理根必是整数.

于是，求多项式有理根的问题归结为下述运算： 1) 找出自由项的全体因子和最高项的全体因子； 2) 用这些因子组成既约分数； 3) 把分数代入多项式中进行验算. 在这一步可以使用霍纳方法. 如果验算的结果都是否定的，则表示多项式没有有理根.

求线性因子这个笨活宜从 ±1 开始. 计算 $f(1)$ 和 $f(-1)$ 并不困难. 现若整数 c 是多项式 $f(X)$ 的根，则 $f(X) = (X-c)q(X)$, 其中 $q(X) = b_0X^{n-1}+b_1X^{n-2}+\cdots+b_{n-1}$. 从霍纳方法直接推出 $b_i \in \mathbb{Z}, 0 \leqslant i \leqslant n-1$. 因此，商

$$\frac{f(1)}{c-1} = -q(1), \quad \frac{f(-1)}{c+1} = -q(-1)$$

也应该是整数. 这就表明, 如果 $d \in \mathbb{Z}$ 且 $d|a_n$, 但 $\dfrac{f(1)}{d-1}$ 和 $\dfrac{f(-1)}{d+1}$ 中至少有一个不是整数的话, 则显然 $f(d) \neq 0$. 当然, 即便 $\dfrac{f(1)}{d-1}$ 和 $\dfrac{f(-1)}{d+1}$ 都是整数, 也不能保证 $f(d)=0$.

例 9 $f(X)=X^5+2X^4-15X^3-2X+6$. 我们有 $f(1)=-8, f(-1)=24$. 因子 $d=\pm 6$ 立即被排除, 因为 $d+1$ 不整除 24. 另一方面, 对于 $d=2$ 有 $\dfrac{f(1)}{2-1} \in \mathbb{Z}$ 且 $\dfrac{f(-1)}{2+1} \in \mathbb{Z}$, 但 $f(2) \neq 0$. 对于 $d=-3$, 情形相仿. 事实上, 整数根是 6 的因子 3.

习 题

1. 设 $f(X)=a_0X^n+a_1X^{n-1}+\cdots+a_n$ 是一个 n 次实系数多项式. 证明: 知道了多项式 $f(X), X^nf\left(\dfrac{1}{X}\right), f(-X), X^nf\left(\dfrac{-1}{X}\right)$ 的正根的一个上界, 就得出了多项式 $f(X)$ 的正根和负根的下界和上界.

2. 用上题的记号, 设 $a_0>0, m$ 是使 $a_m<0$ 的最小指标, B 是负系数的绝对值的最大值. 证明对于多项式 $f(X)$ 的任何正实根 c 都有

$$c \leqslant 1+\sqrt[m]{\frac{B}{a_0}}.$$

提示: 当 $x>1$ 时, 使用估计式

$$f(x) \geqslant a_0x^n - B\frac{x^{n-m+1}-1}{x-1} > \frac{x^{n-m+1}}{x-1}[a_0x^{m-1}(x-1)-B].$$

3. 设 P 是零特征域, $a \in P$. 证明任意 n 次多项式 $f \in P[X]$ 满足公式 (泰勒公式)

$$f(X)=f(a)+\frac{1}{1!}f'(a)(X-a)+\frac{1}{2!}f''(a)(X-a)^2+\cdots+\frac{1}{n!}f^{(n)}(a)(X-a)^n.$$

提示: 对形式表达式 $f(X)=\sum b_i(X-a)^i$ 逐项求导 k 次然后令 $X=a$.

4. 证明: 若 n 次实多项式 $f(X)$ 的首项系数 $a_0>0$ 且 $f(a)>0, f'(a)>0, \cdots, f^{(n)}(a)>0$, 那么 $f(c)=0, c>0 \Rightarrow c<a$.

提示: 利用习题 3.

5. 利用笛卡儿符号法则求多项式 X^5-X^2+1 和 X^3-6X-9 的判别式的符号 (参阅第 1 段末尾的注记).

6. 多项式 $X^5-X-1, X^3+aX+b \in \mathbb{Q}[X]$ 可能有公共的复根吗? 回忆 (见 §1 的习题 11) 多项式 X^5-X-1 在 $\mathbb{Q}$ 上是既约的.

7. 证明自由项 $w \neq 0$ 的多项式 $f(X)=X^5+uX^4+vX^3+w \in \mathbb{R}[X]$ 的根不可能全是实的.

提示: 转换到**相关多项式** $X^5f\left(\dfrac{1}{X}\right)$ 再利用 §1 的公式 (12) 和 §2 的公式 (8).

8. 如果任取 $x \in \mathbb{R}, f(x) \geqslant 0$, 则实多项式 $f(X)$ 可以表示成

$$f(X)=g(X)^2+h(X)^2$$

的形状, 其中 $g, h \in \mathbb{R}[X]$.

提示：利用定理 1，把 $f(X)$ 分解成形如 $(X+a)^2+b^2$ 的因子并使用从关系式 $|p+iq|^2|r+is|^2 = |(p+iq)(r+is)|^2$ 推出的恒等式

$$(p^2+q^2)(r^2+s^2) = (pr+qs)^2 + (ps-qr)^2.$$

9. 独立求出 3 次和 4 次多项式的稳定性准则．当 $n=4$ 时，把它写成不等式的形式：

$$a_1 > 0, \quad a_4 > 0, \quad a_1a_2 > 0, \quad a_3(a_1a_2 - a_3) > a_1^2a_4.$$

提示：$f(X) = X^3+aX^2+bX+c = (X^2+\alpha X+\beta)(X+\theta)$，其中 $a = \alpha+\theta, b = \beta+\alpha\theta, c = \beta\theta$，且 $\alpha, \beta, \theta \in \mathbb{R}$. $f(X)$ 的稳定性与一对多项式 $X^2+\alpha X+\beta, X+\theta$ 的稳定性等价，即与不等式组 $\alpha > 0, \beta > 0, \theta > 0$ 等价．容易验证，这组不等式等价于不等式组 $a > 0, b > 0, c > 0, ab-c > 0$. 对于 4 次多项式类似地进行讨论．

10. 既约有理分式

$$\frac{f(X)}{g(X)} = \frac{3}{X+2} + \frac{1}{(X-1)^2} - \frac{2}{X-1} + \frac{X-3}{X^2+1},$$

它的分子，多项式 $f(X)$ 有实根吗？

11. 证明 $\mathbb{Q}$ 上的既约多项式 $f(z) = z^3-7z-7$ 的三个根都是实的且位于开区间 $(-2,4)$ 中．用牛顿法计算它的正根，要求精确到十进小数点后第三位．

12. 利用鲁歇定理 (定理 5) 证明，多项式 $f(z) = z^5+5z^2-3$ 在单位圆内有两个根而在圆周 $|z|=1$ 和 $|z|=2$ 之间的环中有三个根．

13. 多项式 z^4+12z^2+5z-9 有多少个实根？

14. **勒让德多项式** $P_0(X) = 1, P_1(X) = X, \cdots, P_n(X), \cdots$ 可由递推公式

$$mP_m(X) - (2m-1)XP_{m-1}(X) + (m-1)P_{m-2}(X) = 0$$

定义．证明：

a) $P_n(1) = 1, \quad P_n(-1) = (-1)^n$;

b) $\{P_n, P_{n-1}, \cdots, P_0\}$ 是 $P_n(X)$ 在闭区间 $[-1,1]$ 上的斯图姆组；

c) $P_n(X)$ 在开区间 $(-1,1)$ 中有 n 个彼此相异的根．

附录　关于多项式的公开问题

以下用星号标记的问题，截止到 2000 年以前的数学文献中事实上都没有解答，其余的问题原则上解决了，但所用的手段或者是非代数的，或者是非初等的. 当然，对于未解决的问题而言，使用任何手段都是有益的.

陈述问题的同时附有少量评注，以便帮助读者理解事情的本质并开阔视野. 此处列出的参考文献很少.

1.* 雅可比猜想　设 $f_1,\cdots,f_n\in\mathbb{C}[X_1,\cdots,X_n].\partial_j f_i=\dfrac{\partial f_i}{\partial X_j}$ 是多项式 f_i 对第 j 个变元 X_j 的偏导数，即作用偏导子 (此处也是通常的偏微分算子) 所得的函数 (见第 6 章 §1 的习题 9). 设 $f_i(0,\cdots,0)=0,1\leqslant i\leqslant n$. 用下述公式引入新变量 $X_1',\cdots,X_n'$:

$$X_1'=f_1(X_1,\cdots,X_n),\cdots,\quad X_n'=f_n(X_1,\cdots,X_n).$$

多项式映射 $F=(f_1,\cdots,f_n):X_i\to X_i',1\leqslant i\leqslant n$, 定义了多项式代数 $\mathbb{C}[X_1,\cdots,X_n]$ 的一个自同态 (到自身的同态). 其雅可比矩阵

$$J(F)=\begin{pmatrix}\mathcal{D}_1f_1 & \cdots & \mathcal{D}_nf_1\\ \cdots & \cdots & \cdots\\ \mathcal{D}_1f_n & \cdots & \mathcal{D}_nf_n\end{pmatrix}$$

可逆，当且仅当行列式

$$\det J(F)=\begin{vmatrix}\mathcal{D}_1f_1 & \cdots & \mathcal{D}_nf_1\\ \cdots & \cdots & \cdots\\ \mathcal{D}_1f_n & \cdots & \mathcal{D}_nf_n\end{vmatrix}$$

是一个非零常数 (即 $\mathbb{C}^*$ 中的元素), 该行列式叫作**雅可比行列式**, 一般来说是一个多项式.

如果 F 是自同构，即若存在多项式 $g_1,\cdots,g_n$, 使得

$$X_1=g_1(X_1',\cdots,X_n'),\cdots,\quad X_n=g_n(X_1',\cdots,X_n'),$$

则易验证雅可比行列式是可逆的. 逆命题是否成立? 换言之, 是否能断定

$$\det J(F) \in \mathbb{C}^* \Longrightarrow F\text{是自同构?} \tag{*}$$

这就是 **雅可比猜想**, 对 $n \geqslant 2$ 的所有情况都没有解决.

马上可以看到代数 $\mathbb{C}[X_1, \cdots, X_n]$ 有两个特殊的自同构群. 群 GL_n 由所有的非退化线性变换组成, 而群 B_n 的元素是下述形状的 "三角" 多项式变换的合成:

$$X_i \mapsto X_i + t_i(X_{i+1}, \cdots, X_n), \quad 1 \leqslant i \leqslant n, \quad t_i \in \mathbb{C}[X_1, \cdots, X_n].$$

不难验证, 这些变换是可逆的. 例如当 $n=3$ 时, 有

$$\begin{cases} X_1' = X_1 + t_1(X_2, X_3), \\ X_2' = X_2 + t_2(X_3), \\ X_3' = X_3. \end{cases}$$

因而

$$\begin{cases} X_1 = X_1' - t_1(X_2' - t_2(X_3'), X_3'), \\ X_2 = X_2' - t_2(X_3'), \\ X_3 = X_3'. \end{cases}$$

每一个保持纯量不变的自同构是否可以由 GL_n 和 B_n 中元素的合成得到? 预料当 $n \geqslant 3$ 时此事不真. 更有甚者, Nagata**猜想** 说, 哪怕对下述具体的自同构 $F: X_i \mapsto X_i'$, 答案也是否定的, 其中

$$\begin{cases} X_1' = X_1 - 2X_2(X_1X_3 + X_2^2) - X_3(X_1X_3 + X_2^2)^2, \\ X_2' = X_2 + X_3(X_1X_3 + X_2^2), \\ X_3' = X_3. \end{cases}$$

我们发现, $J(F) = 1$, 并且

$$\begin{cases} X_1 = X_1' + 2X_2'(X_1'X_3' + X_2'^2) - X_3'(X_1'X_3' + X_2'^2), \\ X_2 = X_2' - X_3'(X_1'X_3' + X_2'^2), \\ X_3 = X_3'. \end{cases}$$

存在着许多不同的途径进入雅可比猜想 (代数几何的, 函数论的), 把它们综合在一起取得了部分的成效. 令 $\deg F = \max\limits_{1\leqslant i\leqslant n} \deg f_i$. 若 $n=2$ 且 $\deg F \leqslant 150$, 则问题 (*) 的答案是正面的. 此外, 精确到 GL_n, 证明中只要考察下述多项式

$$f_i = X_i + h_i(X_1, \cdots, X_n), \quad 1 \leqslant i \leqslant n,$$

其中所有的分量 h_i 都是三次齐次型 ($\deg h_i = 3$), 而对于 $H = (h_1, \cdots, h_n)$, 雅可比矩阵 $J(H)$ 是幂零的, $(J(H))^n = 0$. 在归纳过程中, 变元的个数 n 比开始时增加.

关于雅可比猜想，已有结果的详情可以在综述文章中找到：Bass H., Connell E. H., Wright D. Jacobian conjecture // Bull. Amer. Math. Soc. 1982. V. 7, No. 2. P. 287~330.

2.* 判别式问题 (E. A. Гори н)　设

$$f(X) = X^n + a_2X^{n-2} + \cdots + a_n$$

是首一多项式，系数 $a_i, 2 \leqslant i \leqslant n$, 是 $\mathbb{C}$ 上的有理函数 (即 $\mathbb{C}(z)$ 中的分式).假设多项式 f 的判别式 $D(f)$ 恒等于 1. 系数 a_i 有可能不全为常数吗？

已知下述事实.

a) 如果全部系数 a_i 的奇点 (极点) 是 0 和 ∞(在既约分式 $a_i = \dfrac{p}{q}$ 中，或者分母 q 被 z 整除，或者 $\deg p > \deg q$), 则 $a_i, 2 \leqslant i \leqslant n$, 是常数.

b) 如果 $n = 3$ 或 $n = 4$, 则所有的 a_i 是常数.

当 $n = 3$ 时, 问题转化为求方程 $u^3+v^3 = 1$ 的有理解 (见第 6 章 §2 第 4 段), 该方程是三次费马方程的简化. 如果 $f^n+g^n = h^n$, 其中 $f, g, h \in \mathbb{C}[z]$, 且 g.c.d.$(f, g, h) = 1$, 则已知当 $n > 2$ 时，多项式 f, g, h 是常数. 当 $n = 4$ 时，利用费拉里的立方预解式. $n = 5$ 的情况尚无答案.

3. 多项式环的二元生成问题　从数学文献中了解的 Абъянкар-Мох 定理断言，如果 $\mathbb{C}[f(z), g(z)] = \mathbb{C}[z]$, 即多项式 f, g 生成整个多项式环，则：

i) 多项式对 f, g 分离 $\mathbb{C}$, 即若 $z_1 \neq z_2 \Rightarrow f(z_1) \neq f(z_2)$ 或 $g(z_1) \neq g(z_2)$;

ii) 导数 $f'(z), g'(z)$ 没有公共零点.

该定理至今没有简单的证明. 需要找到初等的方法.

从各种证明中的一个已解决问题：若多项式对 f, g 满足性质 i),ii), 则或者 $\deg f | \deg g$, 或者 $\deg g | \deg f$.

Зайденберг-Лин 的定理 (DAHCCCP.1983.T.271,No.5) 同样指出，若多项式对 $f, g \in \mathbb{C}[z]$ 分离 $\mathbb{C}$, 则

$$\mathbb{C}[f(z), g(z)] = \mathbb{C}[(z-c)^k, (z-c)^l],$$

其中 $c \in \mathbb{C}$, 而 g.c.d.$(k, l) = 1$. 特别地，方程组 $f'(z) = 0, g'(z) = 0$ 最多只有一个解. 这个论断比 Абъянкар-Мох 定理要强. 对 Зайденберг-Лин 定理也需要找到初等证法.

接下来我们指出，将 $\mathbb{C}$ 换成 $\mathbb{R}$ 是不可能的. 看来也没有将两个多项式 f, g 拓广成三个多项式 f, g, h 或更多的类似定理.

4.* 临界点和临界值问题　(B. Sendov, S. Smale, A. И. Кострикин, Э. Б. Винберг). 设 $f(z)$ 是复多项式，$\Theta_f = \{\theta \in \mathbb{C} | f'(\theta) = 0\}$ 是 f 的 **临界点集**,(即导数 $f'(x)$ 的零点集).f 在临界点 $\theta \in \Theta_f$ 处的值 $f(\theta)$ 叫作 **临界值**.

a) 如果次数 $n \geqslant 2$ 的多项式 $f(z)=\prod_{k=1}^{n}(z-c_k)$ 的所有的零点 (根) 都在单位圆 $D_1=\{z\in\mathbb{C}\,\big|\,|z|\leqslant 1\}$ 内，证明对于每一个 c_k, 圆 $\{z\in\mathbb{C}\,\big|\,|z-c_k|\leqslant 1\}$ 至少含有一个临界点.

这一方向的结果可见下文： Miller M. J.// Trans. AMS. 1990. V.321, No. 1. P. 285~303.

有关多项式临界点的一般代数几何的概念在下述著作中有所阐述： Marden M. Geometry of polynomials.——Providence, R.I.:AMS, 1966.

Сендов 问题明确了这本书中的一个已知结果，根据这个问题，包含有多项式 $f(z)$ 的全部零点的任意圆 D_r, 亦包含有其导数的全部零点. 假设 $f(z)$ 的所有零点都是实的，并再看一遍第 6 章 §4 定理 3 的证明，此事很容易验证.

b) 证明 若 f 是满足 $f(0)=0, f'(0)\neq 0$ 的 n 次复多项式，则

$$\min_{\theta\in\Theta_f}\left|\frac{f(\theta)}{\theta}\right|\frac{1}{|f'(0)|}\leqslant\frac{n-1}{n}.$$

Smale 证明了存在临界点 θ, 使得

$$\frac{|f(\theta)|}{|\theta f'(0)|}\leqslant 4,$$

即给出了所需的最差估值常数. 对于次数 $n\leqslant 4$ 的多项式，问题已解决. 常数 $\frac{n-1}{n}$ 不能改进，考察例如多项式 $f(z)=z^n-\frac{n-1}{n}z$ 证实了这一点.

c) 我们用符号 C_n 记所谓 **保守多项式** $f(z)=z^n+a_1z^{n-1}+\cdots+a_{n-1}z$ 的集合，其定义性质为 $f'(\theta)=0\Rightarrow f(\theta)=\theta$. 这样，保守多项式可看作一个映射 $f:\mathbb{C}\to\mathbb{C}$, 它使坐标原点和自己所有的临界点保持不变.

已知 $|C_n|=\begin{pmatrix}2n-2\\ n-1\end{pmatrix}$(Tischler D.Complexity.1989), 所以对于 n 次保守多项式，转化为证明不等式 $|f'(0)|\geqslant\frac{n}{n-1}$ 的 Smale 问题在原则上解决了. 但对此需要掌握 C_n 中多项式的明确的描述，目前只了解到 $n\leqslant 6$. 较弱的不等式 $|f'(0)|>1$ 对任意 $f\in C_n$ 成立.

一个非常有趣的问题是，研究保守多项式零点和不动点的几何.

d) 设 f 是实系数 n 次多项式，且有实临界点集 ($\Theta_f\subset\mathbb{R}$). 所有这种多项式的集合记作 $\mathcal{P}_n$. 我们把每一个 $f\in\mathcal{P}_n$ 按下述法则对应于一个向量 $\mathrm{cr}f\in\mathbb{R}^{n-1}$. 设 $\theta_1,\cdots,\theta_{n-1}$ 是 f 的递增排列的临界点 (按重根计算). 则 $\mathrm{cr}f=(f(\theta_1),\cdots,f(\theta_{n-1}))$ 是一个临界值的向量. 显然，向量 $(c_1,\cdots,c_{n-1})\in\mathbb{R}^{n-1}$ 对某个多项式 $f\in\mathcal{P}^n$ 形如 $\mathrm{cr}f$, 仅当 $(-1)^k(c_k-c_{k+1})\geqslant 0$ 对所有的 k 成立，或反之， $(-1)^k(c_k-c_{k+1})\leqslant 0$ 对所有的 k 成立，也就是说，序列 $c_1,\cdots,c_{n-1}$ 是“锯齿状”的.

用非常复杂的方式证明了，所有的锯齿状向量 $c=(c_1,\cdots,c_{n-1})$ 对应于一个多项式 $f\in\mathcal{P}_n$，使得 $\mathrm{cr}f=c$ 这样的多项式 f 精确到自变量的线性替换 $x\mapsto ax+b, a,b\in\mathbb{R}, a>0$，是唯一的.

是否存在这一问题的初等证明？

5. 牛顿方法的整体收敛问题 (Smale S.//Bull.Amer.Math. Soc.1985.V.13,No.2) 我们把复数集 $\mathbb{C}$ 连同附加的符号 ∞ 理解为 **黎曼球面**S，而将映射 $z\mapsto\dfrac{P(z)}{Q(z)}$，其中 P,Q 是多项式，理解为 S 到自身的 **有理自同态**.

给定一个 n 次复多项式 $f(z)$，**牛顿有理自同态**$N_f:S\to S$ 由我们已知的第 6 章 §4 第 7 段公式 (12) 定义：

$$N_f(z)=z-\frac{f(z)}{f'(z)}.$$

复数 $\zeta\in\mathbb{C}\subset S$ 叫作 N_f 的 **不动点**(即 $N_f(\zeta)=\zeta$)，当且仅当 ζ 是多项式 f 的零点，在这种情况下，导数 N_f' 在 ζ 点的值恰为 $N_f'(\zeta)=\dfrac{n-1}{n}$，是我们在第 4 段 b) 中遇到过的数.

计算多项式 f 的根 (零点) 的牛顿方法可以看作 N_f 的 **迭代映射**:$N_f^0(\zeta_0)=\zeta_0$，$\zeta_m=N_f(\zeta_{m-1})=N_f^m(\zeta_0)$. 在我们今天的数学文献中，$(N_f,S)$ 被当作 **动力系统**，并且很好地运用发达的技巧对它进行研究.

已经指出 $|N_f'(\zeta)|<1$，这就意味着存在点 ζ 的邻域 U，使得任取点 $z\in U$，$\lim\limits_{m\to\infty}N_f^m(z)=\zeta$. 这时 ζ 叫作 **汇点**(或关于 N_f 的 **吸引不动点**)，而开集 $B=\bigcup\limits_{m\geqslant0}N_f^{-m}(U)$ 叫作汇点 ζ 的 **区域**. 点 $\alpha\in\mathbb{C}$ 叫作关于 N_f 的 **周期为 k 的汇点**，若 $N_f^k(\alpha)=\alpha$ 且 $|(N_f^k)'(\alpha)|<1$. 当 $k>1$ 时，点 $\alpha,N_f(\alpha),\cdots,N_f^{k-1}(\alpha)$ 是两两不同的，同时在包含有 α 的某个邻域 U 内，对 $z\in U$ 的迭代 $N_f^i(z)$ 走向围绕 $\alpha,N_f(\alpha),\cdots,N_f^{k-1}(\alpha)$ 的渐近循环不给出不动点. 这就意味着，如果 N_f 具有周期 $k\geqslant2$ 的汇点，那么谈论 N_f 对 "几乎所有的 $z\in\mathbb{C}$" 的整体收敛性就没有意义. 当 $n\geqslant3$ 时，构造一个任意次数 $n\geqslant3$ 的多项式，使 N_f 有周期汇点是很容易的. 例如当 $n=3$ 时，$f_0(z)=\dfrac{1}{2}z^3-z+1$ 就是一个这样的多项式. 充分接近 f_0 的多项式也具有这些性质.

当 $n=2$ 时，情况完全两样. 设多项式 $f(z)=z^2+az+b$ 有两个不同的根 ζ,η，并设 L 是垂直于线段 $[\zeta,\eta]$ 且经过它的中点的直线. 那么直接验证可知 (一个很好的习题) 任取点 $z\in\mathbb{C}\backslash L$，即可以取几乎所有的点，序列 $\{N_f^m(z)\}$ 收敛于 ζ 或 η. 例如设 $f(z)=z^2-d, d\in\mathbb{R}, d>0$. 这时虚轴 $L=i\mathbb{R}$ 经过线段 $[-\sqrt{d},\sqrt{d}]$ 的中点. 由于任取 $t\in\mathbb{R}, N_f(t)\in\mathbb{R}$，且 $N_f(it)=it+\dfrac{t^2+d}{2it}=i\left(t-\dfrac{t^2+d}{2t}\right)\in i\mathbb{R}$，则 $N_f^m(it)\in i\mathbb{R}$. 于是，从纯虚数 $z=it$ 开始，我们永远不会遇到直线 L，自然地，不能得到逼近于 $\sqrt{d}$ 或 $-\sqrt{d}$ 的牛顿方法. 反之，唯一的条件 $\mathrm{Re}z\neq0$ 保证了这一逼近，尽管可能不

是非常迅速.

另一个评注. 变量替换 $z \mapsto \alpha z$ 将 n 次多项式 f_0 变为多项式 $f_1(z) = b_0 z^n + \cdots + b_n$, 当 α 充分大时, 可以使 $|b_0| \geqslant |b_k|$ 对所有的 k 成立. 其次, 任取 $\lambda \in \mathbb{C}^*$, 多项式 f_1 和 λf_1 的零点和临界点是相同的. 类似地, $N_{\lambda f_1} = N_{f_1}$, 这就意味着, 在牛顿方法的讨论中, f 可以取自系数的模不超过 1 的标准多项式的集合 $\mathcal{P}_n(1)$. 根据第 6 章 §3 引理 3, 多项式 $f \in \mathcal{P}_n(1)$ 的全部零点在圆 $D_2 = \{z \in \mathbb{C} \,|\, |z| \leqslant 2\}$ 中. 设

$$B_f = \{z \in \mathbb{C} \,|\, \lim_{m \to \infty} N_f^m(z) = \zeta(z), f(\zeta(z)) = 0\}$$

是 N_f 的所有汇点的区域之并. 直接地说, 在对 f 应用牛顿方法时, B_f 是收敛区域.

集合 $\mathcal{P}_n(1)$ 的特性使我们有可能仅限于交集 $B_f \bigcap D_2$ 的考察, 其面积记作 $v(B_f \bigcap D_2)$. 关系式

$$A_f = \frac{v(B_f \bigcap D_2)}{v(D_2)} = \frac{v(B_f \bigcap D_2)}{4\pi}$$

可以看作从 D_2 随机地取点时, 牛顿方法收敛的概率. 我们已经靠近了主要问题的公式. 令

$$A_n = \min_{f \in \mathcal{P}_n(1)} A_f.$$

当然 $0 \leqslant A_n \leqslant 1$. 根据上述评注, $A_2 = 1$, 而当 $n \geqslant 3$ 时, $A_n < 1$.

需要证明, 对于任意 n, 不等式 $A_n > 0$ 成立. 将 A_n 看作 n 的函数也是很好估计的.

暂时甚至连 $A_3 > 0$ 也没有证明.

"还有许多问题我愿意告诉你们,
但是你们现在尚不能接受."

摘自福音书 Иоанн 16:12

名词索引

J

K

L

M

N

O

P

Q

R

S

Z

补 充 文 献[1]

1. Под реДакцией Кострикина. А И Сборник задач по алгебре. —М.: Факториал, 1995. （《代数习题集》）
2. Курош А Г. Курс высшей алгебры. —ю-е изд. —М.: Наука, 1971. （《高等代数教程》）
3. Фаддеев Д К. Лекции по алгебре. —М.: Наука, 1984. （《代数学讲义》）
4. Шафаревич И Р. Основные понятия алгебры. —М.: ВИНИТИ, 1986. （《代数基本概念》）

希腊字母表

$A\alpha$	$B\beta$	$\Gamma\gamma$	$\Delta\delta$	$E\varepsilon$	$Z\zeta$
alpha	beta	gamma	delta	epsilon	zeta
$H\eta$	$\Theta\theta$	$I\iota$	$K\kappa$	$\Lambda\lambda$	$M\mu$
eta	theta	iota	kappa	lambda	mu(myu)
$N\nu$	$\Xi\xi$	Oo	$\Pi\pi$	$P\rho$	$\Sigma\sigma$
nu(nyu)	xi(ksee)	omicron	pi	rho	sigma
$T\tau$	$\Upsilon\upsilon$	$\Phi\varphi$	$X\chi$	$\Psi\psi$	$\Omega\omega$
tau	upsilon	phi	chi(ki)	psi	omega

①以上四种教材或参考书的作者都是俄罗斯 (前苏联) 著名的代数学家，他们的工作在代数学领域的影响广泛且深远，在国际上享有崇高的声誉. —— 译者注.

［Ｇｅｎｅｒａｌ Ｉｎｆｏｒｍａｔｉｏｎ］
书名＝代数学引论　第一卷·基础代数　第二版
作者＝Ａ·И．柯斯特利金著
页数＝２３６
ＳＳ号＝１１８６５４００
出版日期＝２００６．１２